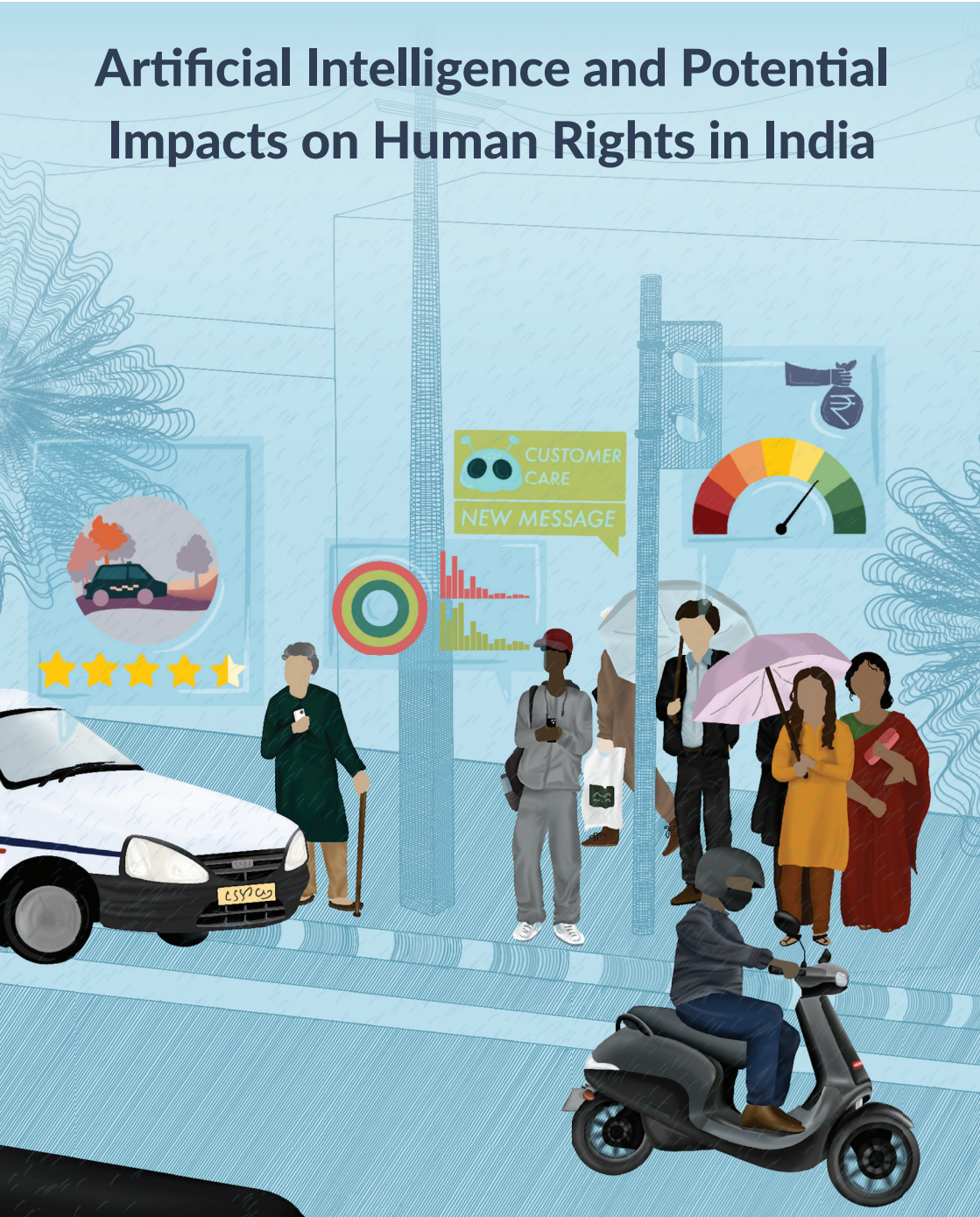
aapti institute

Funded by the European Union

B+HR BUSINESS AND HUMAN RIGHTS | ASIA

UNDP

Artificial Intelligence and Potential Impacts on Human Rights in India



Artificial Intelligence and Potential Impacts on Human Rights in India

Report

May 2022

aapti institute

Aishani Rai, Vinay Narayan & Dr. Sarayu Natarajan

Authors

Acknowledgements

This report was produced by Aapti Institute, commissioned by the United Nations Development Programme (UNDP) under the Business and Human Rights in Asia programme, funded by the European Union. This document should not be considered as representative of the European Union's official position. The views expressed in this publication are those of the authors and do not necessarily represent those of the European Union, the United Nations, including UNDP, or the UN member States.

In addition to contributions from the wider Aapti team, this report also draws upon the expertise of numerous academic and industry experts, practitioners, and workers. We are grateful for their input during interviews and feedback sessions.

Editor: Yana Banerjee-Bey | **Report design:** Meher Rajpal

Cover Illustration: Shubhangi Karia

Aapti is a public research institute that works on the intersection of technology and society. It examines the ways in which people interact and negotiate with technology both offline and online.

This is a work of independent research, commissioned by the **United Nations Development Programme (UNDP) under the Business and Human Rights in Asia programme, funded by the European Union**

Artist note on cover page illustration

The notification icons were modelled on existing design interfaces of various apps so that they are at once familiar to any reader. There are four icons representing the tech lives of as many sectors. First, a star rating notification for gig work that is common to taxi and delivery services. Second, a customer care chatbot used in retail, replacing human resource personnel. Third, credit score meters – signalling the finance industry. And, finally, an activity graph used by health apps. While the data displayed in these notifications is personalised to users, they remain standardised.

Table of Contents

Glossary

Term	Definition
AI automation *(IBM, n.d.)*	The most complex level of automation is artificial intelligence automation. The addition of AI means that machines can "learn" and make decisions based on past situations they have encountered and analysed.
AI based credit scoring *(Raso et al., 2018)*	Usage of artificial intelligence to assess the credit risk of a potential borrower, analysing vast amounts of data from many sources.
AI bias *(PWC, 2021)*	An occurrence where the output of algorithmic processing results in systematic prejudices against certain groups of persons.
Artificial Intelligence *(Allison-Hope and Hodge, 2018)*	Intelligence exhibited by machines including both "machine learning" (an approach to achieve Artificial Intelligence or AI), which uses algorithms to parse data, learn from it, and then make a determination or prediction, and "deep learning" (a technique for implementing machine learning), which is inspired by understanding the biology of our brains.

Automated Decision Making *(ICO UK, n.d.)*	The process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Automated decision-making often involves profiling, but it does not have to.
Gig work *(Aapti analysis)*	Gig work involves temporary jobs, typically in the service sector, where the worker is engaged as an independent contractor or freelancer. In most cases, the allocation of tasks is mediated by a platform company.
Predictive Analytics *(Deloitte Insights, 2019)*	Predictive analytics is a branch of advanced analytics which in the realm of healthcare transforms patient care, both at individual level and on a cohort scale, by evaluating historical and real-time data.
Profiling *(UK GDPR)*	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Executive Summary

Introduction

Not only is the role of artificial intelligence (AI) growing across sectors, this growth is in turn propelling economic progress massively. It is driven by easily available data, growing digitisation, capital flows, and efficiency gains from use of AI. The impact of AI is diverse and wide, and affects a range of stakeholders – the State, businesses, consumers and workforces.

For instance, accelerated economic growth promotes State interests in serving the economic well-being of citizens. Business models are built on deployment of AI, and its usage in workflows facilitates efficiency and profitability. Consumers routinely avail of unique and enhanced services facilitated by AI. Workers interact with AI on a day-to-day basis, given that AI is integrated into workflows – smoothening flow of operations.

However, AI deployment is not free from concerns of human rights (HR) risks. Given that consumers and workers represent the human dynamic that interacts with technology, they experience risks, particularly in the sectors of financial services, healthcare, retail and gig work. Human rights risks are further exacerbated for marginalised and vulnerable populations, who may be without access to technology or without redress in cases of abuse. Understanding the intersection of AI with human rights is critical for meaningful protection of human rights, job creation, and the propagation of an engaged and equitable digital public. Further, it is imperative for businesses to understand this intersection given that rights-respecting businesses drive sustainable economic growth and increased levels of trade and investment, as envisaged by the B+HR Asia programme goals. A robust understanding of AI and business and human rights pushes us one step closer towards achieving the broader Sustainable Development Goals' 2030 Agenda.

We anchor this research on a two-part framework – identification of human rights risks and suggested strategies for mitigation. The identification of risks is based on an understanding of international covenants such as the Universal Declaration of Human Rights, the International Covenant on Economic,

Social and Cultural Rights, and the International Covenant on Civil and Political Rights, and national legal documents such as the Indian Constitution and various pieces of statutory legislation. Mitigation strategies are aligned with the three-pillar 'Protect, Respect and Remedy' framework of the United Nations Guiding Principles on Business and Human Rights (UNGPs) outlining the duty of the State to protect human rights and the responsibility of businesses to respect the human rights of those affected adversely due to their operations.

Given that India seeks to position itself as a dynamic global economy attracting trade and investment, this study is timely – aiming to enable effective adoption of AI technologies within a human rights framework presented under the UNGPs.

The UNGPs lens on AI: Value for stakeholders

Engagement with issues relating to AI and human rights can unlock value for all stakeholders. For the State, the twin goals of social and economic inclusivity are achieved. It enables protection of citizens in accordance with prevailing legal frameworks, and is aligned with ongoing initiatives of the State such as 'Digital India' and 'Responsible AI' that seek to create ethical frameworks for AI deployment. It provides a facilitative environment for steady and sustainable economic growth through long-term investments. For businesses, a reduced human rights risk profile is conducive to attracting foreign investments. It creates a stable work environment, enhancing productivity. Additionally, it may lower the headline risks – associated with negative coverage around critical incidents – for organisations. Citizens can benefit from AI-enabled services free from harms such as exclusion, misuse of data, and privacy intrusion that impinge on human rights. The UNGPs framing equalises power equations between business conglomerates, their consumers, and workforces.

Company policy, regulatory frameworks and AI: Unpacking sources of human rights risks

The impacts of AI across sectors cannot be isolated from company policies and regulatory frameworks. Human rights risks are not solely a product of a problematic technology product or service, but are greatly aggravated due to underlying company policy and regulatory frameworks. AI technologies mirror company policies and choices – as company preferences are embedded in technology during its development. Outcomes of technology-based processes are thus a reflection of decisions taken at corporate level. Regulatory frameworks are foundational to guiding company policy and their absence may foster environments with a disregard for human rights – either due to the absence of standards or due to lack of redressal mechanisms. Women and economically disadvantaged communities experience ill effects as biases replicate in AI systems, exacerbating human rights risks.

Anticipating and mitigating human rights risks from AI use

Currently, in India, a few sectors are experiencing significant proliferation in use of AI. Increasing usage entails added human rights risks in the absence of regulatory mechanisms. For instance, credit scoring in financial services leads to risks to privacy and exclusion harms; lack of grievance redressal affects access to finance and borrowing, and financial well-being. Predictive analytics in healthcare leads to likelihood of bias and discrimination, loss of patient and doctor autonomy, and loss of data privacy resulting in inferior patient care. AI automation in retail leads to job loss and threatens worker autonomy. AI intermediation in gig work imposes work in poor conditions without social security protections and an absence of adequate grievance redressal, translating into worker exploitation.

Fortunately, there is a growing number of incentives to encourage

business to address human rights risks posed by AI. Our understanding of actions to mitigate these risks has been informed by interviews conducted with a wide range of experts and business leaders and then consolidated into broad recommendations. The Annexures comprise a policy brief for the State (Annexure A) and sector-wise risk assessment toolkits for businesses (Annexure B) that propose implementable and workable pathways for risk mitigation.

Our findings emphasise that State regulation is crucial to ensure businesses take measures to mitigate AI's adverse impacts on human rights. The State must enforce existing norms and regulations and extend applicability to AI, wherever possible. The Government of India should also identify gaps in enforcement tools and in legislation. The government can provide for guidance of the private sector to ensure its responsibility to respect human rights in AI usage is well understood. Lastly, the government should ensure coherence across ministries either promoting or regulating use of AI.

Indian businesses stand to benefit from paying attention to the correlation of business incentives and human rights. A milieu where businesses respect rights can drive the sustainability of economic growth. Businesses need to adopt policies and due diligence practices to ensure they are preventing adverse human rights impacts. They should also communicate measures in force to avert harms. Further, businesses should also consider a range of remedial action for when their use of AI results in harms. They should scrutinise the impact of AI on consumers and workers, and maintain a minimum stipulation of human intervention and oversight across sectors for AI deployment.

01 /

Introduction

The pandemic has increased the demand for digitised services, and consumer and worker lives are transforming drastically with increased adoption of artificial intelligence (AI). AI growth has been driven by easily available data, growing digitisation, capital flows, and efficiency gains from use of AI, propelling massive economic growth. A range of stakeholders is benefitted due to AI deployment – the State, businesses, consumers and workforces. The State benefits from accelerated economic growth and increased use of technology which align with its broader objective of 'Digital India'. AI is simply a new technology for businesses to integrate in their products and services, and presents new opportunities for businesses to expand products, services and markets. Further, its usage in workflows facilitates profitability. Consumers avail of unique and enhanced services facilitated by AI. Workers interact with AI on a day-to-day basis, given that it is integrated into the workflows – smoothening flow of operations.

Human engagement with technology is visible in the areas of consumption and work. We engage with AI to access products and services; simultaneously, workflows are increasingly moderated by using AI to drive productivity gains. Consequently, the risks may be appraised in relation to these two types of engagement. Consumers grapple with the risks of bias and discrimination, loss of privacy, erosion of autonomy and harms of market exclusion. Workers are often primarily threatened by risk of job loss. Poor working conditions and absence of grievance redressal are other risks that perpetually stress workers.

Thus, understanding the intersection of AI with human rights is critical for meaningful protection of human rights, for job creation, and for the establishment of an engaged and fair digital public. The goal of the United Nations Development Programme (UNDP) Business and Human Rights in Asia (B+HR Asia) programme is to enable sustainable economic development across Asia, and to help businesses consider and manage human rights and the impacts of their operations. Mapping the human rights impact of AI technology deployed by businesses in India is crucial, given that the nation seeks to position itself as a dynamic global economy attracting international trade and investment. A robust understanding of AI and the United Nations Guiding

Principles (UNGPs) on Business and Human Rights framework pushes us one step closer towards achieving the Sustainable Development Goals' 2030 Agenda. This study seeks to enable effective adoption of the UNGPs framework in the Indian context, by engaging key stakeholders, promoting public diplomacy and proffering rights-based solutions.

Importance of the study

Deployment of AI in businesses aligned with the UNGPs framework impacts three stakeholders – the State, businesses and society – and addressing AI-related human rights concerns has manifold gains for all three.

Understanding the UNGPs framework will enable the State to protect citizens and build an inclusive digital economy (Pillar 1, UNGPs – State Duty to Protect Human Rights). From the economic perspective, it accelerates steady, sustainable and equitable economic growth, setting the stage for lucrative long-term foreign direct investment (FDI) and green-field investments. Moreover, it aligns with ongoing efforts by the Government of India (GoI) towards creating ethical frameworks for AI usage through its 'Responsible AI' initiatives, and could facilitate setting up of an oversight body to govern AI (Pillar 3, UNGPs – Access to Remedy).

A better grasp of the intersection between AI and human rights can enable businesses to meaningfully create jobs and well-being (Pillar 2, UNGPs – Business Responsibility to Respect Human Rights). Businesses are then better positioned to detect problematic practices and adopt appropriate guardrails and regulatory protections. In terms of solutions, appropriate incentives such as sandboxes and clear liability regimes propel innovation. A reduced human rights risk profile attracts foreign investments for market players.

Deployment of AI in accordance with the UNGPs framework can build a thriving digital public by addressing harms such as exclusion, misuse of data, and privacy intrusion that impinge on constitutionally guaranteed fundamental rights and underlying human rights. This study seeks to suggest pathways that level the power dynamics between

business conglomerates and their diverse consumers (Pillar 3, UNGPs – Access to Remedy).

Civil society has significant potential for mapping the ethical frameworks of AI adoption for businesses. Given the lack of clarity on its role, we aim to underscore its significance in bolstering the State in fulfilling its duty to protect human rights and make businesses respect human rights.

It is in the best interests of businesses, societies, and governments to invest in understanding these harms and in building measures to address them in an effective and timely manner. We believe that there is a need for a disaggregated understanding of business and human rights issues to fully realise the gains of AI. Given the trajectories of AI adoption in India, it is indeed an opportune moment to frame a balanced rights-based approach and a corresponding liability regime.

Approach

This paper builds on existing literature to identify the human rights risks due to AI deployment by businesses. We employed a combination of desk research and interviews with key stakeholders in the ecosystem. Given that deployment of AI penetrates deeply across numerous business sectors and is utilised in diverse ways, we adopted a nuanced approach to streamline the study by appraising critical sectors while ensuring a productive and wide inquiry, with a measure of generalisability.

The approach is outlined as follows:

a. mapping the *unique effects* on
b. specific groups of population *(consumers and labour force)*
c. based on the *specific type of AI* deployed by businesses

Adopting this streamlined approach enabled us to pinpoint distinctive effects on consumers and the labour force in each sector identified, increasing the utility of the study's insights for the State and businesses.

Simultaneously, the wider coverage of sectors, taking into account types of interaction with AI (i.e. as consumers and as workers), allows the findings to be applicable to other contexts.

Our approach led us to focus on four key sectors – financial services, healthcare, retail and gig work – by building a robust analysis of the human rights impact of AI deployment.

As we deep dived into the intersection between AI deployment by Indian businesses and the UNGPs framework, we identified areas for further research in India.

Documentation of AI risks is generalised across sectors though its impacts across sectors are varied, depending on the type of AI and the nature of the sector. Further, the impact of AI is varied with harms being aggravated for some population segments, especially women. An absence of evidence-based studies in these areas in India proffers scope for further research that would enable stakeholders to glean magnified insights into the intersection of AI deployment by business and its impact on human rights and allow them to push more vigorously for adoption of human rights protection in businesses.

Structure of the paper

The following chapter outlines approach and methodology. Chapter 3 examines the use of AI and its intersection with the UNGPs on Business and Human Rights. A sectoral approach is adopted. Chapter 4 presents the human rights risks in each sector. The last chapter proposes pathways to mitigate risks identified in each sector, outlining the role of the State and businesses.

02 /

Approach

Methodology

This aims to identify harms and build solutions around use of AI by businesses within the UNGPs framework, relying on a combination of desk research and interviews of experts.

This is built on the following methodologies:

A Problem-centred expert interviews and analysis

This method provides the quickest access to specific nuances of the sector as the interviewees have privileged access to information. Their insights are solution-oriented, given that the people interviewed are in control of strategies and are integral to the decision-making process.

a. Problem centred interview: A problem-centric approach helped to understand the subjective perceptions and underlying objective evidence of these experts.

b. Narrative and thematic analysis of interview data: This step required us to develop a narrative based on the stories presented by each expert. Their stories were reformulated, taking into account the context of each case and the experts' diverse experiences.

c. Data coding and organization: This step focused on analysing the data from the interviews methodically.

B Doctrinal analysis and non-doctrinal desk research

a. Doctrinal analysis: Doctrinal analysis required us to understand the legislation and regulatory frameworks around AI and human rights. International human rights instruments (UNGPs) and national human rights legislation were scanned to ascertain the various human rights which are at stake due to deployment of AI in business.

> ***b. Non-doctrinal analysis and research:*** Non-doctrinal research allows us to understand the implications of the legislation from the perspective of other disciplines, with the aim being to integrate those perspectives into the current framework.

We imagined the implementation of the method in the following approach:

1. Mapping existing human rights risks that may emerge through desk research (literature review, doctrinal analysis) and are supported by the expert interviews.

2. Outlining suggested pathways for mitigation through expert interviews and supported multistakeholder consultations.

Sector identification

Four sectors were identified for further analysis owing to the unique effects on consumers and labour force, based on the specific type of AI deployed by businesses. Viewing the human rights impact from a bipartite lens of consumers and labour force, we were able to cover the supply and demand areas of business. From that starting point, for consumers, we looked at financial services and healthcare; for the workforce, we looked at retail and gig work.

Consumer lens

We identified two non-technology, consumer-facing sectors from the viewpoint of AI impact on consumers. The financial services and healthcare sectors are promising, given that they fall within the business-to-consumer realm. Selecting non-technology, consumer-facing sectors enabled us to focus keenly on the primary goal of this study, pivoting around mapping the human rights impact. The focus on non-technology sectors is significant as they present immense opportunity to steer social change, but also entail capability to produce social harms (Allison-Hope and Hodge, 2018).

Our preliminary research, inclusive of a combined approach of quantitative sectoral ranking and qualitative subjective analysis, inclined towards financial services and healthcare as potential sectors for the study. Figure 1 depicts the quantitative mapping of the top five sectors assessed.

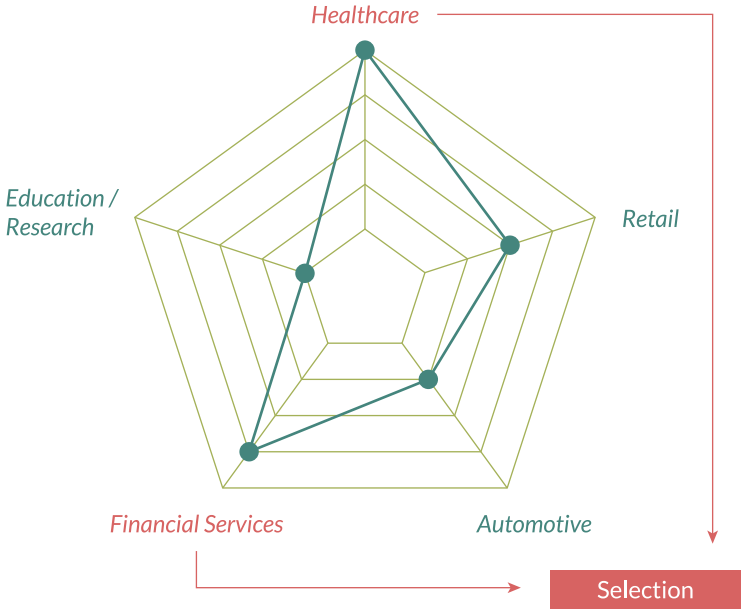


Figure 1: Sector Selection from Consumer Lens

We assessed non-technology, consumer-facing sectors based on a set of quantitative parameters such as the AI market share/value of each sector, current and future trajectories of AI demand, and the potential AI consumption impact in each sector. Combining the findings, we mapped the relevance of those sectors, and applied a subjective lens. This inclined us towards financial services and healthcare, given the indispensable nature of these services. Health and finance are key to survival, directly impacting our rights to physical and economic well-being. Our analysis in toto indicates that the use of AI is set to increase manifold in these critical sectors, with maximum human rights implications on consumer-citizens.

Labour force lens

In order to understand the implications of AI deployment by businesses for the labour force from a human rights perspective, we looked at two types of AI, viz., AI-enabled automation and AI-intermediated work. Both sectors are labour-intensive, but AI adoption poses different problems for the workforce in either sector, as shown in Figure 2.

We assessed labour-intensive sectors such as manufacturing, agriculture, retail and gig work with a view to identifying possible sectors of study to understand the threat AI automation poses in terms of job loss and other attendant human rights. As delineated in Figure 2, key parameters for selecting a sector included current adoption of AI in the sector, appetite for further AI adoption, and the role of AI automation within the sector.

Criteria for selection

- Must be labour-intensive: manufacturing, agriculture, retail, platform economy considered
- Is an emerging sector: pace of AI adoption
- Subjective element of feasibility

AI Automation - Retail sector

- ***AI already widely adopted:*** 5th most in terms of AI by industry.
- ***Increase in future AI adoption:*** 85% retail insiders believe that AI improves organizational efficiency.
- ***Automation disproportionately impacts retail:*** Potential for automation in tasks done by retail salespersons is at a high of 47%

AI intermediated work - Gig work

- ***AI adoption:*** Platform companies use proprietary algorithms to intermediate work
- ***Employment Potential:*** The gig economy has the potential to serve up 90 million jobs in India
- ***Low Labour Standards:*** Most (>80%) gig companies rate extremely poor for labour standards

Figure 2: Sector Selection from Labour Lens

03 /

Intersections of sectoral AI use with UN Guiding Principles on Business and Human Rights

This chapter explores the intersections of AI use in each sector (through relevant Indian and global examples) with the UN Guiding Principles on Business and Human Rights framework, to identify specific themes for exploration.

Before proceeding to sectoral AI use, it is useful to understand the meaning of human rights. As defined by the United Nations, human rights refer to "rights we have simply because we exist as human beings – they are not granted by any State. These universal rights are inherent to us all, regardless of nationality, sex, national or ethnic origin, color, religion, language, or any other status. They range from the most fundamental – the right to life – to those that make life worth living, such as the rights to food, education, work, health, and liberty".

This report relies on the United Nations Guiding Principles on Business and Human Rights framework, the world's most authoritative such entity, as a guide to how AI should be deployed across business sectors. The framework outlines the duty of the State to protect human rights and, equally, the responsibility of businesses to respect human rights.

Sectoral intersection of AI and UNGPs on Business and Human Rights

Automated decision-making and predictive analytics: Understanding the use of AI in financial services and healthcare

Since the COVID-19 pandemic has increased reliance on technology, this has served to necessitate corresponding input in designing technologies to be equitable and inclusive (Natarajan & Sharma, 2021). A rights-based approach primes AI design and deployment to be inherently inclusive as it adopts a universal standard of human rights as an essential condition.

The share of AI-enabled services and products in the financial sector stands at 9.6% (Thomas, 2020), and at 1.9 % in healthcare (Thomas, 2020). In a survey, 94% of healthcare leaders affirmed an intention to

invest in AI (Philips India, 2021) and AI investments in the healthcare and finance sectors increased globally by 44% and 28%, respectively (McKinsey, 2020). These numbers reiterate the criticality of AI in these sectors.

In India, AI is viewed as a transformational solution to bridge the vastly uneven doctor-patient ratio, especially during the pandemic when the sector grappled with issues of cost, quality and accessibility of services (NASSCOM, 2021). AI in healthcare harbours potential to add USD 25 billion to USD 30 billion to India's GDP by 2025 (NASSCOM, 2021). Similarly, in the financial sector, the pandemic has increased the demand for digitalised services and businesses are increasingly relying on AI to enhance customer experience (Jha, 2021). The potential AI consumption impact for the health and financial sectors globally, on a scale of 1 to 5 has been determined to be 3.7 and 3.3, respectively, underscoring its value for businesses (PWC, n.d.).

The scope for AI integration into healthcare services in India is massive. Outside of research and development, big pharmaceutical companies are innovating newer tech-enabled services to combat diseases such as malaria and diabetes (P. Rao, n.d.).

Transformational opportunities exist in delivery of critical health services such as radiology and antibiotic resistance, to name a couple, which have high consumption across geographies (P. Rao, n.d.). An initial inquiry into the predictive healthcare sector reveals that inaccuracies in analysing the underlying patient need, ingrained bias and discrimination lead to poorer patient care as well as loss of consumer agency and autonomy, gravely impacting human rights such as those to quality healthcare, life and liberty, and freedom of choice (Raso et al., 2018; WHO Guidance, 2021).

Preliminary insights related to financial services highlight that use of credit scoring shows that the lack of algorithmic transparency and information asymmetries between the financial service provider and the consumer deepen power imbalances, leading to market exclusion and exacerbating chilling effects on consumer behaviour (Raso et al., 2018). These concerns impinge on consumer rights to equality, privacy, and effective remedy. For instance, it is well documented that communities of colour and women are often discriminated against by AI-enabled services when seeking financial credit (Rice & Swesnik, 2013).

Triangulating the effects of AI deployment by businesses on human rights onto consumer and citizen rights informs well-rounded governance at corporate level, as well as an empowered and knowledgeable civil society to support communities they serve.

Job automation and AI-intermediated work: Exploring the use of AI in retail and gig work

While use of AI technologies can create job opportunities in areas such as data-labelling (Natarajan et al., n.d.), it can have deleterious effects on the labour force in a number of traditional and growing sectors. The most significant threat of AI automation in traditional industries such as retail, agriculture and automobiles is that of job loss. Along with this, AI automation can also pose additional hazards including loss of control over their data for workers and a risk of dehumanisation (Miller, 2021).

The retail industry was among the worst-hit by the COVID-19 pandemic, and there is now a spike in retail brands looking to adopt digital transformation initiatives (Roy, 2021). Retail ranks fifth in India in terms of AI adoption market share, behind IT, technology, finance and engineering (RBSA, 2021). Other labour-intensive sectors such as the automobile industry and agriculture tech rank much lower, with significantly less AI adoption. Further, retail is also witnessing a high demand for adoption with 85% of retail companies planning to use intelligent automation for supply chain planning by 2021 (IBM, n.d.). Another major area of AI automation in the retail space is the use of chatbots for customer service as over 70% of chatbot conversations are expected to be with retail conversational AI systems by 2023 (Dilmegani, 2020). There is fear of job loss due to AI automation among retail employees as only 26% of them are supportive of AI adoption (the lowest amongst all industries surveyed) (KPMG, 2020).

Analysing the ways in which AI automation in the retail sector affects the labour force is therefore significant, and can inform strategy for businesses to structure their AI adoption to accommodate human rights.

AI-intermediated work has been heralded for its ability to create job opportunities, but it comes with its own set of perils. Preliminary research has shown that worker surveillance, atomisation of work (fragmentation of work into smaller tasks – breaking up of a task into 'microtasks'), and an absence of social security benefits are some of the most common complaints (Rathi & Tandon, n.d.). Despite the rhetoric of flexible work, platforms often lock in gig workers through algorithm-driven payment structuring that can incentivise staying online on the app for longer, or create disadvantages for workers who decline jobs while available (Meyers, 2021). Indeed, courts in the UK have recognised that the only way for Uber drivers to increase their earnings is by working longer hours while constantly meeting Uber's measures of performance[1].

The classification of platform workers as independent contractors rather than traditional employees also allows platforms to sidestep social security obligations. While many jurisdictions globally are working towards expanding social security protections to cover platform workers, the situation in India continues to be precarious. While the Code on Social Security, 2020, does mention increased social security benefits for platform workers, there is a great deal of ambiguity in the definitions used (Sarkar, 2020) and a lack of adequate protections for workers (Chami & Sanjay, 2020).

AI-intermediated work is witnessing a meteoric rise and with more people entering the gig work space, it is now imperative to analyse this sector. Mapping the human rights issues in this sector can help in advising State policy to ensure platform businesses function with adequate respect for rights.

[1] Uber BV and others (Appellants) v Aslam and others (Respondents) [2021] UKSC 5

	Type of AI	Effect	Sector
Consumers	Profiling and Automated Decision Making	Erosion of market access	Financial services
	Predictive Analysis	Erosion of consumer agency	Healthcare
Labourforce	AI automation	Loss of job	Retail
	AI intermediated work	Worker surveillance	Gig work

Figure 3: Mapping of AI deployment by businesses and the human rights-related impact on consumers and labour force

Sources of human rights: Exploring the intersection of AI and the UN Guiding Principles on Business and Human Rights framework

The concept and span of human rights have evolved from a broad range of doctrinal and normative approaches. It is essential to start by streamlining our understanding of human rights. Appraising international and domestic sources allows for consideration of a wide range of human rights.

For this study, we adopted the three-pillar 'Protect, Respect and Remedy' framework of the United Nations Guiding Principles on Business and Human Rights, focussing on the State's duty to protect and business responsibility to respect human rights at risk due to AI deployment across the four selected sectors:

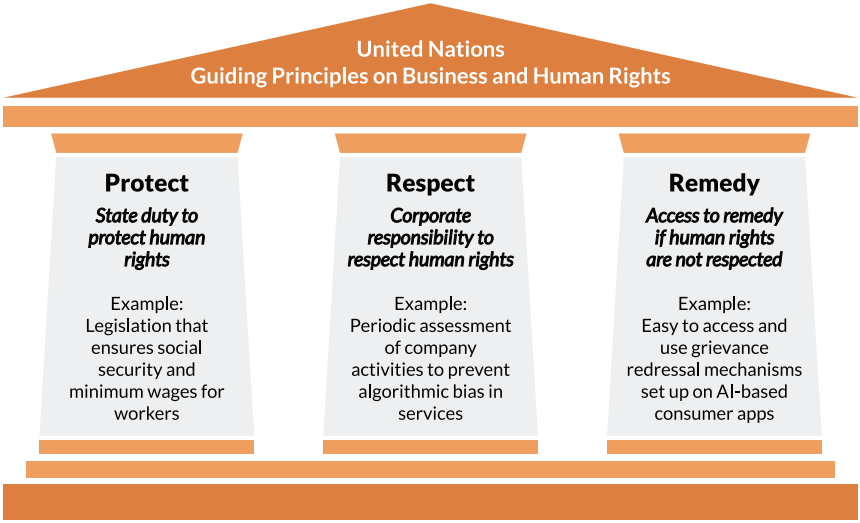


Figure 4: Intersection of AI use in businesses and UNGPs' 'Protect, Respect and Remedy' framework

In addition to the UNGPs' three-pillar outline, the human rights framework also derives from international covenants such as the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, as well as domestic legal documents such as the Indian Constitution and statutory legislation.

Figure 5: Business and human rights frameworks across international covenants and Indian legal documents

04 /

Key Findings

Intersection of AI, company practice and governance

AI effects across sectors cannot be isolated from company policies and regulatory frameworks

We may see the effects of use of AI by businesses on human rights as emerging from the AI technology itself, but the consequences for human rights are further amplified by company policy and the regulatory framework. Experts across sectors emphasise that human rights risks are not a result of the technology alone, but arise from the interplay of technology, company policy and regulation.

Expert interviews reveal that harms stemming from AI are exceptional, given the technology's ability to affect a vast number of people at a time without violations being detected in the first instance. Human rights risks are further exacerbated for women and the economically disadvantaged as biases existing in traditional models creep into AI, amplifying the impact.

Figure 6 illustrates AI deployment and its intersection with company policy and regulatory framework along with examples across sectors.

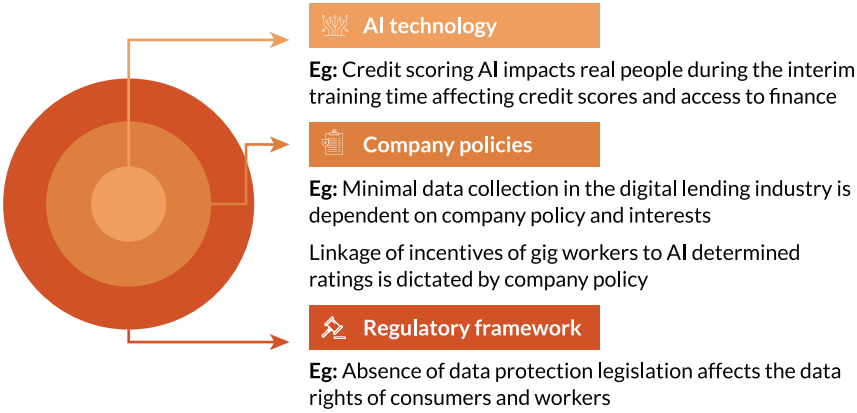


Figure 6: Intersection of AI, company policy and regulatory framework

Company policy

> ***"Algorithmic decision-making is a term that is often used by companies to hide/obfuscate what is a deliberate company policy."***
>
> - Platform Work Researcher

Businesses distinguish themselves from the technology they adopt by emphasising the inherent limitations of AI and that making AI explainable is beyond their technical capability, and that AI is a black box. However, the concept of Responsible AI is increasingly being explored by companies, suggesting that AI reflects corporate values and vice versa (AIRS Working Group, n.d.).

The experts interviewed reiterated that businesses do play a critical role in development of AI and its working. Technology primarily interacts with the company and most of these business strategies are private, thereby limiting State intervention with respect to the technical nuances of the technology. This may relate, for example, to the encoding of the minimum number of work hours in platform work applications. AI thus mirrors business policy, preferences and choices.

Regulatory framework

> ***"It is time for State intervention and regulation. We need to create an environment for discussing ethics."***
>
> - Healthcare Investor (a)

> ***"The State has two primary duties – creating a regulatory framework and ensuring enforceability."***
>
> - General Counsel for a healthcare firm

Human rights risks are not solely a product of the interaction between AI technology and the business. The UNGPs provide that the State and

businesses have shared but distinct responsibilities to ensure that human rights are protected and respected in business operations. The primary duty of the State to protect human rights lies in framing laws and regulation, and setting guidelines for business actions and decisions. Lack of regulation makes the State a stakeholder contributing to human rights risks. For instance, predatory digital lending apps, which have no incentive to mitigate human rights risks, exist because of an absence of regulation to prevent their operation.

Legal and regulatory frameworks guide AI deployment by businesses and influence core company functioning and data protection/ privacy practices. The European Union, in its proposal for an AI-related legal framework, considers regulation essential for consumer trust (European Commission, 2021).

Sector-wise deep dives

Financial services and AI-based credit scoring: Risks to privacy, financial access and grievance redressal

The utility of AI in financial services is immense, given its interaction across operations – from hiring of employees to operationalising Know Your Customer (KYC) norms, facilitating responsible investment, guiding insurance decisions, and determining creditworthiness of consumers. Of these, AI-based credit scoring and lending are noteworthy. AI-based credit lending finds empirical relationships between new factors based on the collection of large datasets and the creditworthiness of the consumer (Klein, 2019).

AI-based credit scoring offers notable potential to tap new market segments. This is especially the case given that only 15% of Indian households have access to formal channels of credit, making India one of the most underserved credit markets of the world (IFMR Finance Foundation,

2017). Potential consumers primarily face the hurdle of a lack of credit history, depriving them of scope to access credit (Chandran, 2021). Mitigating consumer risks associated with AI-based credit scoring through innovative regulatory frameworks is imperative to boost digital credit lending to USD1 trillion by 2023 in India (Chandran, 2021).

Understanding AI-based credit scoring

AI-based credit scoring is structured to rely on vast amounts of data which is then processed, leading to outputs. The amount of data collected by lenders is huge and its nature varied. It can range from social media profiles to utility bills, or through tracking of every activity such as what is eaten and worn, and other seemingly irrelevant and mundane aspects (Basu, 2020). This reflects that all data in any form can be integrated into a credit model (Klein, 2019).

As indicated in Figure 7, diverse input data is utilised to produce outputs. The data is used to profile consumers as creditworthy or non-creditworthy based on the assignment of a credit score. Depending on the outcome, the algorithm decides whether the consumer is eligible for a loan.

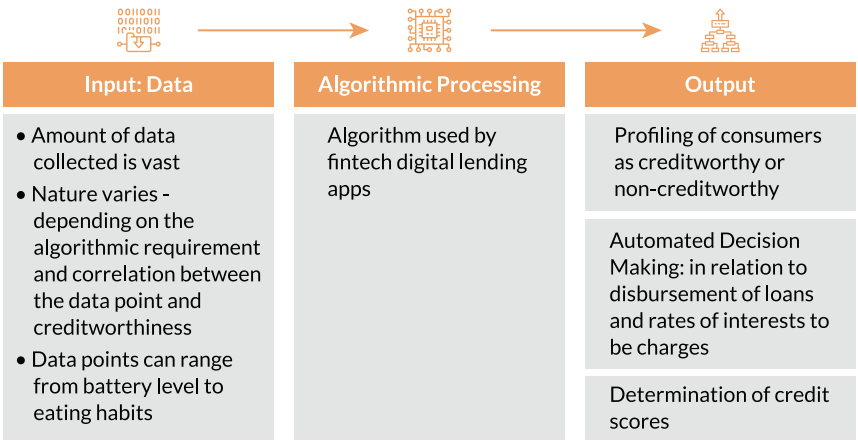


Figure 7: AI-based credit scoring in financial services is basically a flow from data to output

Element in AI processing	Breakdowns	Specific HR risk
Data collection	Lack of informed consent during inference cycles	• Risk to Privacy • Risk to financial access and wellbeing
Metrics	Lack of relevant metrics resulting in false assumptions leading to bias and inaccuracy in determination of creditworthiness	• Risk to financial access and wellbeing • Risk to life, dignity and safety
Interim training time	Lack of business awareness of impact of AI during training period	• Risk to financial access and wellbeing • Risk to life, dignity and safety
Algorithmic opaqueness	Lack of algorithmic transparency and explainability incapacitating consumers of their right to reason of denial of credit	• Risk to remedy and grievance redressal

Figure 8: Each element in AI processing results in breakdowns that lead to specific human rights risks

Apart from understanding financial credit scoring as a flow from data to output, we can also attempt to understand the process through the components of algorithmic processing unique to AI-based credit scoring, as shown in Figure 8.

All steps of AI use have effects on human rights and form a matrix with individual risks. AI-based credit scoring is a result of multiple overlapping factors and elements integral to AI processing. Figure 8 simplifies the concept – showing each element corresponding to a particular breakdown that results in a specific human rights risk.

For one, lack of informed consent in the data collection process impinges on the right to privacy. Next, AI-based credit scoring entails reliance on metrics to ascertain the creditworthiness of consumers. Irrelevancy of metrics leads to inaccuracy in creditworthiness

determination, in turn leading to risks to financial access and well-being. Integral to the development of AI is its training period when the technology, though not perfect, is still being utilised, and decisions flowing from it affect real populations (not control or trial groups). Lastly, a common feature of most AI technology is algorithmic opaqueness which in AI-based credit scoring translates into a denial of consumers' right to know the reason for the decision, affecting their ability to seek effective remedy.

Stakeholder mapping

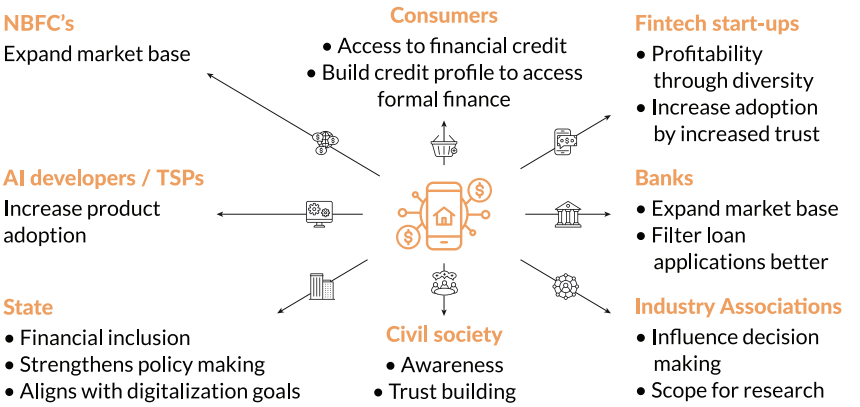


Figure 9: Stakeholder mapping of AI in the financial sector

As suggested by Nobel laureate Muhammad Yunus, access to financial credit in itself is a human right (Raso et al., 2018). It enables realisation of social and economic well-being and is beneficial for numerous stakeholders. For consumers, the primary benefit lies in being able to avail of credit previously denied due to inadequate documentation about their finances and credit history. AI-based credit scoring presents a newfound opportunity for them to build a credit profile and access formal finance, reducing their reliance on informal means of accessing finance which most often lead to debt traps. For business entities such as banks, non-banking financial companies (NBFCs) and fintech start-ups, AI-based credit scoring expands market bases. It enhances efficacy

of core operations such as filtering loan applications more accurately, translating into economic advantages where default rates are reduced (Raso et al., 2018). For the State, broader goals of financial inclusion, especially amongst marginalised and historically disadvantaged communities, are achieved and this aligns with the Digital India mission as well.

Human Rights Risks

Human Rights Risk	Legal Frame
Risk to privacy	• Right to privacy (right to object against Automated Decision Making, right to reasonable inference) (UDHR Article 12, ICCPR Article 17)
Risk to financial access and wellbeing	• Right against discrimination (ICESCR Article 2) • Right to equality (UDHR Article 7, ICCPR Article 26, ICESCR Article 2) • Right to life (financial access) (UDHR: Article, ICCPR: Article 6)
Risk to life, dignity and safety	• Right to life • Right to privacy
Risk to effective remedy and grievance redressal	• Right to effective remedy (lack of contestability) UDHR: Article 2, ICCPR: Article 8

Figure 10: Identification of four human rights risks and corresponding legal basis

Risk 1: Risk to privacy

> ***"Privacy in India is a zero sum game. There is a perception that we need to give up our fundamental right to privacy to access finance, which should not be the case. Service providers lack the understanding that privacy is a first order issue, even amongst lower income households."***
>
> - Policy Researcher (a)

Privacy rights are abused because data collection by lenders is rampant and informed consent before data collection is not sought. Consumers remain unaware of the nature and volume of data collected. Further, there is no regulatory framework to hold business accountable for any abuses that result in unfettered data collection activity.

Informed consent is not sought in India due to multiple factors. First, a study indicates that consumers are unable to comprehend privacy polices due to barriers of language, legal jargon and length (Kulkarni et al., 2019). Of those surveyed, 79.4% of the participants admitted that they did not even read privacy policies (Kulkarni et al., 2019). Evidence suggests that even well-educated people in India are not equipped to understand privacy policies (Bailey et al., 2018). This is worrisome, given that only 8.2% of the population (aged 15 and above) has an education level of high school and above (Bailey et al., 2018). Second, company practices act as a barrier to consumers' right to informed consent. Research indicates that businesses tend to draft privacy policies that are favourable for their interests rather than helping consumers make better and informed decisions (Bailey et al., 2018).

AI-based credit scoring is characterised by rampant data collection policies that flow as a result of the technology, further amplified by company practices and a lack of regulatory framework. The premise of AI-based credit scoring is feeding the algorithms of alternative data. Currently, there exists no restriction regarding the scope of alternative data as all data is considered credit data.

Company practices exacerbate concerns over data collection. A major

fintech company in India reportedly embedded middleware in music and religious verses streaming apps to collect personal data to assess creditworthiness (Sathe, 2019). AI developers have stated that this is a common business practice in India (Sathe, 2019). As highlighted in the expert interviews, there is a fundamental misguided perception of the importance of privacy. Service providers underestimate the value consumers attach to their privacy which leads to rampant data collection, deviating from the core principle of data protection i.e. minimum data collection. Studies show that people from lower socio-economic backgrounds in India do care about their privacy and place a financial value on it (Vidal, 2020).

A lack of regulatory oversight facilitates unscrupulous business practices. Digital lenders currently fall outside the ambit of the Reserve Bank of India (RBI) norms that mandate that only banks need to provide an explanation for credit denial[2]. Digital lenders registered as NBFCs are not legally obliged to provide an explanation, given that the guidelines for the Fair Practices Code applicable to NBFCs do not include a clause on this[3]. Providing an explanation for credit denial entails businesses needing to divulge details of the data relied on for denial. Unexplainable decisions create unaccountable frameworks where digital lenders do not have a need to keep a check on their data collection practices.

Privacy concerns stemming from a lack of informed consent and rampant data collection practices in AI-based credit scoring models constitute a worrisome scenario. First, AI technology is capable of drawing inferences other than determining creditworthiness, which consumers never consented to allow the technology to do. The nature of data collected is based on non-financial metrics such as battery levels, location data and eating habits. However, the volume of such non-financial personal data collected is so vast that when subject to AI processing, data points are correlated to draw inferences about sensitive personal information such as sexual orientation, political and religious views (BEUC Position Paper, 2018). Experts pointed out that consumers do not provide informed consent for inferences to be drawn about their sexuality, and religious and

[2] Reserve Bank of India, Master Circular on Loans and Advances – Statutory and Other Restrictions, July 1, 2015. Available at: https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9902
[3] Reserve Bank of India, Master Circular – Fair Practices Code, July 1, 2015. Available at: https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9823

political affiliations.

These risks are specific to AI-based credit scoring models as traditional models collect only financial data to assess creditworthiness. Unlike AI-based credit scoring models, traditional models do not collect innumerable personal and sensitive data points thereby disabling them to draw inferences other than creditworthiness.

Second, the security risk for Indian consumers is aggravated in the instance of a data breach – glaringly so when compared across financial institutions. A data breach in a bank would compromise one's financial information whereas a data breach of a digital lender's repository would compromise sensitive information such as social media usage, location and contacts history, online behaviour and purchases, in addition to financial information (Internet Freedom Foundation, 2021).

Risk 2: Risk to financial access and well-being

> ***"In finance, there are several behavioural vices that operate on people such as bounded rationality, etc. People are not in a state to decide whether AI based lending is risky or not, given the general limited access to formal sources of loans and presence of unscrupulous money lenders – this is almost like a debt trap people fall into due to misidentification."***
>
> - Policy Researcher (b)

For AI to determine the creditworthiness of an individual, data science engineers need to decide what measurements (or metrics) are useful to track and assess the individual's financial strength or acumen. However, there is no stipulated or authoritative way of determining the best metrics. In fact, excessive reliance on some metrics may lead to inaccurate or even discriminatory results. For example, purchases at inexpensive eating establishments or discount retail outlets may indicate either of two things – that a consumer is frugal and good at saving money or in a desperate situation. When the same metric is used across diverse populations, over-reliance on that metric would lead to skewed results on a massive scale.

This is particularly true given the levels of structural inequality in access to technology. Metrics purely based on online activity are irrelevant to and hence discriminatory towards digitally disconnected populations, leading to loss of opportunity to avail of credit (Chandran, 2021). On the other hand, algorithmic models trained on error-ridden or incomplete data leads to misclassification of individuals as creditworthy, pushing them into debt traps (Deloitte, 2018). In India, lenders target young populations as they are predominantly unbanked. Inability to pay back loans affects the CIBIL scores of these youngsters, undermining their ability to seek finance in future from formal institutions such as banks (Chandran, 2021)[4].

Understanding the reasonableness of metrics is crucial to prevent proxy factors of discrimination creeping into such models. In Figure 11, consumer perceptions of the relevancy of metrics can be ascertained. Most data points collected are seemingly irrelevant/ unimportant to the layman. Even if there exists an algorithmic justification, it must be communicated to consumers by businesses to prevent any proxy factor of discrimination from creeping into such algorithmic models used for accessing financial credit.

Is it fair to use this type of data source to determine who is a good borrower? (Y/N)

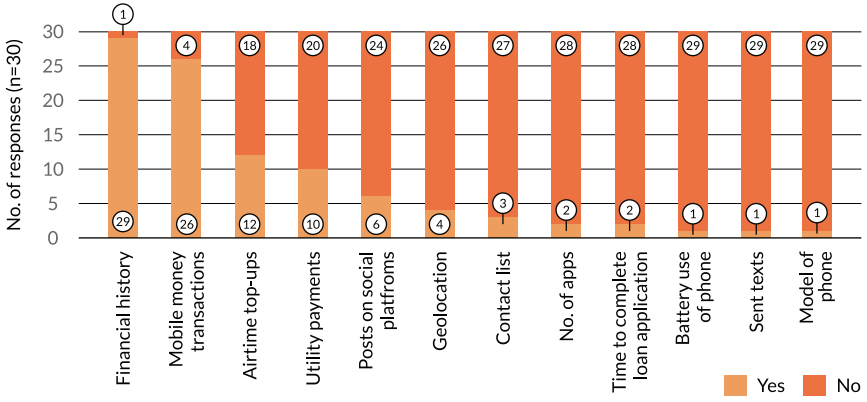


Figure 11: Consumer perceptions of fairness of different data sources that digital lenders could use to determine creditworthiness (Source: Rizzi and Kumari, 2021)

[4] CIBIL score is a three-digit summary of an individual's credit history. Retrieved from CIBIL FAQs. What is a CIBIL score and Report? https://www.cibil.com/faq/understand-your-credit-score-and-report#:~:text=CIBIL%20Score%20is%20a%20three,over%20a%20period%20of%20time

Bias is not unique to AI-based credit models. Even traditional models of scoring are not free from bias. But AI-based credit scoring perpetuates biases at scale, given its opaque and unexplainable nature, and may in fact be often perceived as objective due to automation (Singh & Prasad, 2020). Further, the risk of bias creeping in is higher while relying on AI given that data collection is so vast that AI can discover new proxies for discrimination which were likely not considered by traditional lenders (Klein, 2020). For instance, biases can creep into AI technology due to metrics based on a person's social network. This is also known as network discrimination, where individuals are penalised/ rewarded, based on their personal network circles (Boyd et al., 2014). In the Indian scenario, it translates into discrimination usually based on location as communities are geographically segregated (Internet Freedom Foundation, 2021).

Box 1: AI scores female applicants lower than males

Cases have been reported of AI scoring female applicants lower than males despite similar financial backgrounds. The Goldman Sachs-Apple credit card process showed one such example where the wife was granted a lower credit limit than her husband despite filing joint tax returns and having a higher credit score (Natrajan and Nasiripour, 2019). As reiterated by experts interviewed, women are more likely to face loan rejection if lenders determined creditworthiness based on number of phone contacts, given that men have more social mobility than women in India (Sonne, 2020). The impact is aggravated as women already participate in limited capacities in the economy, and are further trammelled by lack of financing to start their own businesses (Prabhakar and Weber, 2020 (a)).

Expert interview analysis indicates that service providers tend to overlook the effect of AI on consumers during the interim training period. An expert states that adverse effects of AI inaccuracy such as misclassification of real people is unjustified during the time AI trains to attain accuracy rates. This is a problem that arises fundamentally

due to how the AI technology works. Even after the interim training period, if AI credit scoring models operate on historical data with a time lag of two to three months, the results will be inaccurate. For instance, discussions with digital lending stakeholders in India revealed that models that operated in a discontinuous manner failed to consider the altered financial status of the consumer during the pandemic (Dvara, 2021).

Financial harms are also the result of privacy invasions. Consumers are constantly being monitored and data is perpetually being collected. Such unfettered access allows lenders to assess consumer vulnerability and target products and services – for instance, offering a loan when the consumer has just lost their job. The facts are predicted by AI by tracking online activity and drawing inferences (BEUC Position Paper, 2018).

Risk 3: Risk to life, dignity and safety

> ***"There is a risk to life and dignity when AI does not do its job. For instance, I am not sure about the net positive impact of fintech in rural India. The reason for lack of credit is different in rural India than in urban India – it is not merely a lack of credit score but because of an economic condition. There is a need for service providers to understand the underlying economic conditions and apply the right set of metrics."***
>
> - Policy Analyst

There exist two types of lenders – predatory and non-predatory. Predatory lenders charge exorbitant rates of interest, and resort to illegal debt recovery practices such as harassing and threatening the consumer for repayment. These lenders have no incentive to address human rights risks of consumers. On the contrary they are the cause of human rights risks that loom over consumers. Hence this report does not intend to inform predatory lenders about the human rights risks of AI-based credit scoring.

Non-predatory lenders do not resort to unscrupulous debt recovery methods. However, the risk to life looms given that inaccuracy

in prediction pushes borrowers into over-indebtedness, leading to suicide. The risk to life posed by non-predatory lending apps directly stems from the financial harms borne by consumers due to misclassification by AI-based credit scoring technology.

In India, there is no regulation for digital lending thus allowing illegal (predatory) and legal (non-predatory) apps to coexist. Further, in the event that non-predatory apps fail to differentiate themselves from their predatory counterparts, consumers are pushed into the traps of predatory lenders. For instance, a woman attempted suicide when nude pictures were demanded of her when she defaulted on loan repayment. The app was a predatory app that used the same domain name as that of a non-predatory one (Christopher, 2021). Most Indian consumers who fell prey to illegal lending were highly qualified individuals working for multinationals (Christopher, 2021). Given that educated consumers fail to differentiate, the risk for the uneducated population is huge.

With the predatory apps, defaulters face harassment and threat to life, dignity and safety as representatives of the apps resort to unscrupulous methods such as public shaming, demanding nude pictures and sending threatening messages. All this is enabled by the repository of information they collected on the pretext of lending (Internet Freedom Foundation, 2021). One study in India, that analysed comments left by users of digital lending apps, revealed that social circles of the user were contacted by the lender without prior permission (Prabhakar and Weber, 2020 (b)). The user was unaware that phone contacts data provided had actually been collected, or that it would be used as a debt recovery tactic.

Box 2: Women and children more susceptible to risk of life, dignity and safety

The threat to life, dignity and safety is aggravated for vulnerable populations. As noted by an expert, women and children are most susceptible given that they face rape threats and demands for inappropriate pictures.

Risk 4: Risk to effective remedy and grievance redressal

> ***"100 percent transparency is not really possible in AI. But efforts are made to make the AI as explainable as possible."***
>
> - AI Lead, Digital Lending app

Algorithmic invisibility and unaccountability are two pressing factors that hamper effective remedy and grievance redressal for consumers. The consumer is left in the dark about what to contest and whom to challenge.

An explanation of a decision is key to seeking effective remedy and grievance redressal. In the absence of an explanation, consumers cannot question or dispute the decision (Joshi, 2020). In traditional models of credit lending in India, consumers are afforded the right to know the reason for denial of credit, under the RBI norms applicable to banks[5]. However, this right does not extend to algorithmic decisions made by digital lenders. The right must be extended and algorithmic decisions must be explainable to consumers.

The level of explanation that should be prescribed as the ideal threshold is highly complex in algorithmic decision-making. There are numerous constraints entailed in effectuating this. For instance, algorithmic neural networks are highly complex, correlating innumerable data points to appraise creditworthiness, which makes it difficult for developers to understand how the AI arrived at the decision (algorithmic invisibility). Further, experts interviewed noted that businesses do not hesitate to make decisions explainable to consumers but, because of the complexity of AI, sometimes they become undecipherable to the lay person. However, even if algorithms are explainable, businesses hesitate to explain the workings of their algorithms to regulators given the lack of intellectual property safeguards and proprietary concerns.

Unaccountable frameworks are

[4] Reserve Bank of India, Master Circular on Loans and Advances – Statutory and Other Restrictions, July 1, 2015. Available at: https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=990

created as decisions become unexplainable to consumers (why the decision was taken) and regulators (how the decision was taken). Experts noted that businesses become less accountable as they cite reasons of algorithmic invisibility or when they outsource AI development to third party developers.

Healthcare and predictive healthcare analytics: Risks to life, equality, privacy and individual autonomy

AI technology is revolutionising healthcare in unimaginable ways by improving patient outcomes, streamlining caregiving pathways and optimising resources with a more patient-centric approach. AI intersects with the healthcare sector in a multitude of ways, including predictive healthcare, precision medicine, and research and development. Predictive analytics is one such area with immense potential to transform healthcare services by reducing rural patient deaths given that 4,300 people die every day due to poor diagnosis in India (Ray, 2018). In 2019, healthcare analytics accounted for ~10.81% of the digital healthcare market in India (Research and Markets, 2020) and it is expected to reach a value of INR 47.04 billion by 2025, expanding at a Compound Annual Growth Rate (CAGR) of ~20.49% during the 2020-25 period (Research and Markets, 2020). Predictive analytics is a branch of advanced analytics which in the realm of healthcare transforms patient care, both at individual level and at cohort scale, by evaluating historical and real-time data (Deloitte Insights, 2019).

Understanding Predictive Healthcare Analytics

Data is fundamental to the working of AI. Apart from the primary sources of medical data such as electronic health records (EHRs), images, lab results, prescriptions, etc, new data is being generated by wearables and health apps that continuously monitor and collect data about users (Intel, n.d.).

Input: Data	Algorithmic Processing	Output
Medical records submitted by patient comprising of scans, images	Algorithm used by hospitals, as a support tool by doctors	Diagnosis by AI about the prevailing health condition
Continuous monitoring of patients health and behaviour over periods of time	Algorithm used by consumer facing apps	Suggestion of appropriate courses of behavioural action
Medical records and behavioural patterns	Algorithm used by insurance companies	Decision of insurance coverage and premium rates

Figure 12: AI-based predictive analytics in healthcare can be imagined as a flow from data to output

Experts reiterated that there is a need to think of AI differently from other digital technologies. AI is not limited to automation of processes but also uses information in hand to generate new information, as in predictive healthcare analytics.

Predictive healthcare analytics helps us to move closer to personalised care by integrating external factors that affect healthcare with human biology by combining new datasets with the existing sciences of epidemiology and clinical medicine (Gupta, 2018).

Stakeholder mapping

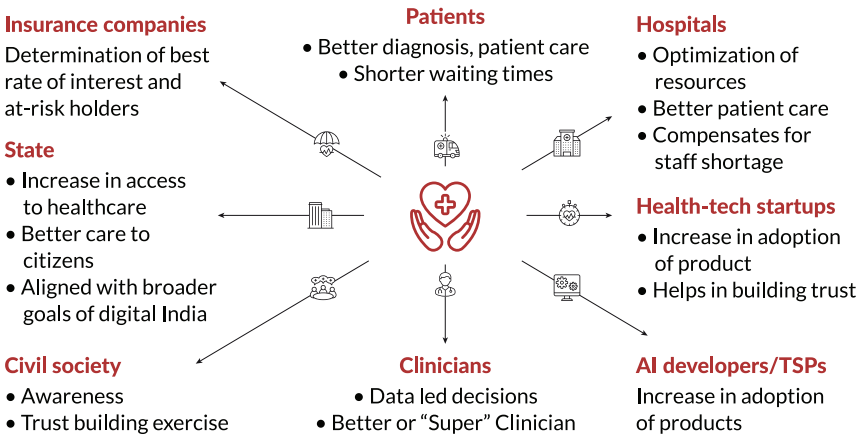


Figure 13: Use of predictive analytics in healthcare entails engagement with several stakeholders, enabling us to move from a reactive to a proactive healthcare system

The advantages of predictive healthcare analytics are multifold for key stakeholders in the caregiving pathway. The Indian healthcare system has limited resources, contributing to longer queues and fragmented care for patients. Further, Indians are known to be non-compliant in adopting preventive healthcare measures, as indicated in a study by THB, an Indian clinical intelligence firm, which revealed that Indian diabetic patients visited their doctors only once or twice a year as against the recommended three to four times a year (Haritas, 2019).

Thus, for the individual patient, it enhances care and curbs costs by improving diagnosis and reducing the need for readmissions, respectively. Since the doctor-patient ratio stands at 1:1457 in India, doctors are able to spend only about two to five minutes per patient – increasing the probability of errors and misdiagnosis (Balaji, 2020). For clinicians, it thus acts as a tool that improves caregiving ability by providing evidence-based decision-making and allowing the clinician to spend more time on critical cases. For hospitals, resources are optimised which allows for care

to be given to the right patient at the right time. On a societal level, it helps State machinery to bolster health systems by identifying and understanding population healthcare trends, compensating for the lack of healthcare staff and infrastructure (Intel, n.d.), further resulting in savings in the healthcare economy (Parry & Aneja, 2020). For low and middle income countries like India, predictive healthcare analytics accelerates access to quality healthcare (Giordano et al., 2021; Parry & Aneja, 2020; Raso et al., 2018).

Human Rights Risks

Human Rights Risk	Legal Frame
Likelihood of bias and discrimination	• Right to Life (quality of life) (UDHR: Article 3, ICCPR: Article 6) • Right against discrimination (ICESCR: Article 2) • Right to equality (UDHR: Article 7, ICCPR: Article 26, ICESR: Article 2)
Loss of individual autonomy (patient and doctor)	• Right to individual freedom of choice, autonomy (UDHR: Article 18, ICCPR: Article 18)
Loss of data privacy	• Right to privacy (UDHR: Article 12, ICCPR: Article 17)

Figure 14: Identification of three human rights risks and corresponding legal basis

Risk 1: Likelihood of bias and discrimination

> ***"Inadequate data about certain populations leads to adverse outcomes. AI is as effective as the data that is collected to train the algorithm and there is a need to retrain the algorithm as the population changes."***
>
> - Healthcare Investor (a)

Risk of bias and discrimination arise from issues related to data quality. Expert interview analysis indicates three primary reasons as cause for biased and discriminatory datasets – lack of diverse datasets, lack of continuous algorithmic training, and presence of untrustworthy sources.

Populations in India will be particularly vulnerable to biased and unfair algorithms as it is a low and middle income country characterised by a lack of regulation, technical expertise and existing social biases against minority groups (Fletcher et al., 2021). When data about certain populations does not exist in sufficient quantities, it leads to uninformative predictions for minority populations, leaving predictions applicable to majority populations (Gianfrancesco et al., 2018). Misdiagnosis is the primary adverse health outcome of biased datasets. The consequence of inadequate datasets for vulnerable populations is not limited to misdiagnosis, but is further aggravated where concerns of accessibility to healthcare services arise. For instance, patients of lower socioeconomic status receive fewer diagnostic tests and medication due to under-represented datasets (Arpey, N.C. et al., 2017).

Each country has its own patterns of diseases most commonly prevalent. In India, cardiovascular diseases affect people much earlier than in middle and high income countries (Prasad, 2021). Given that doctors usually diagnose heart attacks based on symptoms experienced by men, any AI developed to diagnose heart attacks will under-diagnose Indian women (Prasad, 2021).

Diverse datasets must not only capture diverse populations but also capture other socio-economic modalities that affect health. Prediction based solely on EHRs fails to capture external factors such as access to housing and transportation facilities that affect health (Gianfrancesco et al., 2018). For instance, an AI tool was developed to identify patients who were likely to miss appointments. In order to compensate for their non-appearance, the hospital would double book (Murray et al., 2020). If such an AI tool were to be applied in India, it would be biased against rural populations. Healthcare facilities in India are concentrated in urban areas and the rural masses are bound to travel long distances by subpar means of transportation, making it difficult for rural patients to frequently turn up for appointments. The inability of the AI tool to consider constraints related

to costs, distance and transportation leads to double booking. Thus, when these rural patients do appear, the doctor ends up spending less time with them.

Lack of data availability arises due to structural issues of digital inaccessibility. For instance, only 14% of Indian adult women owned smartphones in comparison to 37% of adult men (Statista, n.d.). Data in the healthcare sector is also generated from health apps on smartphones that constantly monitor consumer behaviour. As smartphone data comes primarily from men with above-average incomes, over-reliance on this data may distort our understanding of the health needs of women and of poor women in particular.

Given that change in demography is a constant, expert interview analysis indicates that algorithms that fail to capture these demographic changes contribute to biased datasets.

Experts reiterated that data in India, in its current form, is untrustworthy, error-ridden and fragmented ergo biased and discriminatory (WeForum, 2018).

Box 3: Impact of biased datasets would be disproportionate for female populations

From the perspective of gender, the impact of biased datasets would be disproportionate for female populations as indicated in studies. For instance, research indicates that missing data (such as personal information or specific health details/medical history) in EHRs or incomplete EHRs introduce bias towards older female patients (Weber GM et al., 2017). In another study that assessed digital biomarkers for Parkinson's disease, symptoms of male patients were more accurately detected given that only 18.6% of the sample size was female (Lipsmeier, F. et al, 2018).

Risk 2: Loss of individual autonomy (patient and doctor)

> ***"Medical liability regulation just has not caught up with technology."***
>
> - Healthcare Investor (b)

Loss of autonomy is experienced by both doctor and patient due to deployment of AI predictive analytics. Consumer trust is key to adoption of AI in critical services such as healthcare which is directly linked to how explainable and transparent the algorithm is (Parry & Aneja, 2020). Expert interview analysis indicates that inability of the doctor and patient to understand how and why the AI arrived at a particular decision hampers their autonomy, threatening AI adoption.

Shortage of medical staff and lack of regulatory frameworks can lead to AI technology being a primary decision-maker. However, in India, research by the Centre for Internet and Society indicates that assistive AI technology is most likely to be adopted by the medical fraternity without any resistance as compared to AI technology that seeks to replace doctors (Paul et al., 2018). Experts noted that where AI imparts decisions, several issues unfold that ultimately threaten the autonomy of the doctor.

First, doctors become increasingly concerned that conflicting decisions affect their ability to provide satisfactory care as a result of their diminished confidence in the caregiving pathway. Second, independent performance of the doctor can be affected due to diminished attention (Bitterman et al., 2020). For instance, risk-taking behaviour of the doctor may increase due to ambiguous medical liability regimes, leading to misdiagnosis (Parry & Aneja, 2020). Third, there are additional pressures that doctors need to cope with in highly technological environments. They are constantly required to upgrade their skills in relation to reading, interpreting and communicating information from AI systems to patients, apart from understanding themselves why and how the AI arrived at a particular decision (Deloitte Insights, 2019).

Patient autonomy is one of the core principles of medical ethics

(Childress, 2001). Experts pointed out that information asymmetry about AI deployment and ambiguous medical liability regulation affect patient confidence. Focus group discussions (FGDs) with patients who visited a primary health clinic in the United States revealed that patient autonomy was threatened when they were deprived of the opportunity to choose whether AI should be used in the caregiving pathway or not (Richardson et al., 2021). Further, they expressed hesitation over allowing AI to solely undertake healthcare decisions without the ability to understand the rationale behind the recommendations. Additionally, costs and coverage related to medical AI added to their reluctance to resort to AI in their caregiving pathways.

Risk 3: Loss of data privacy

> ***"Keeping the data secure is of utmost importance and its absence will lead to issues of privacy, which is a human rights risk."***
>
> - Founder, healthtech start-up

Lack of data protection regulation acts as a leeway for rampant collection of health data which in itself is sensitive personal data, as stipulated under the Personal Data Protection (PDP) Bill, 2019. Any breach would directly impinge on an individual's right to privacy.

The impacts of unfettered health data collection and its invisible frameworks of usage are grave for patients and users of health apps. AI enables continuous behavioural monitoring and facilitates rampant collection of data through the notice and consent mechanism, aggravating the threat to privacy (Paul et al., 2018). With respect to collection and storage, the recent move by a million people to opt out of the EHR system maintained by the Australian government reflects the inherent lack of trust in storage of health data (Deloitte Insights, 2019). Regarding data usage, patients who participated in FGDs in the United States revealed that inferences drawn by AI would be used by insurance companies to deny coverage or increase premia, indicating that an

invasion into their medical privacy leads to financial harm (Richardson et al., 2021).

Loss of data privacy is an issue exacerbated in consumer facing apps. Experts noted that continuous behavioural monitoring by health apps results in chilling effects when consumers are restricted to expressing themselves in a manner the former desire, affecting freedom of thought, expression and movement. Physical harm is also likely given that many health apps nudge the user in certain directions without their awareness by combining non-contextualised health information and commercial content (BEUC Position Paper, 2018). These human rights risks contribute to a loss of public trust in the benefits of AI in healthcare, likely leading to an 'AI winter' (Morley et al., 2020).

The Sensitive Personal Data and Information Rules, 2011, categorise medical data as sensitive personal data and mandate that consent be obtained from the patient by the body corporate and the patient be informed about the purpose of collection and data transfer. The current legal framework, however, lacks enforcement – resulting in non-compliance with data privacy norms. For instance, a diagnostic laboratory did not take any action to secure sensitive patient medical data against hacks, resulting in data leak of medical records of 35,000 patients (The Indian Express, 2016).

Retail and AI-based automation: Risks to livelihood, standard of living and worker autonomy

AI technology is set to revolutionise the retail sector with applicability at all levels of the value chain – from optimising inventory management to enhancing consumer experience. By 2022, 70% of all consumer interactions will involve emerging technologies such as machine learning and chatbots (Gartner, 2020). The market size of AI in retail exceeded USD 2 billion, and is expected to grow at more than 30% CAGR between 2021 and 2027 (GM Insights, 2020). The trade body and chamber of commerce for the tech industry in India, NASSCOM

(National Association of Software and Service Companies), highlighted in its study the potential of AI to bring about massive disruptive growth in e-commerce and organised retail in India over the next three years (NASSCOM, 2020). In particular, automated store checkouts, robotic warehouse management, AI-based workforce management and chatbots appear to be key areas of AI deployment for retailers.

Understanding AI automation in the retail sector

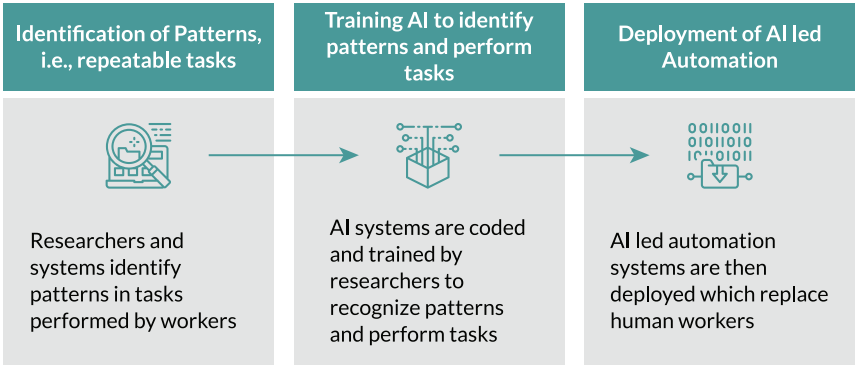


Figure 15: AI systems are trained to perform tasks that require repetition

Deployment of AI-based automation relies on training of AI systems to recognise patterns and carry out repeatable tasks. A high percentage of jobs in the retail sector rely on performance of repeatable tasks, which makes it an ideal sector for AI adoption. The process involves identification of patterns in tasks performed by workers, subsequent training of the systems to recognise patterns in tasks and to perform the tasks, followed by deployment of AI-led automation systems which can perform these tasks at lower cost and higher efficiency than human workers.

> ***"AI-led automation is inevitable, given the big efficiency gains there are for companies."***
>
> - Senior executive at an AI retail solution provider (a)

In addition to this, a number of retailers are also adopting the use of AI-based workflow management software which assists management personnel in tasks such as timesheet, payroll, scheduling and performance management.

Stakeholder mapping

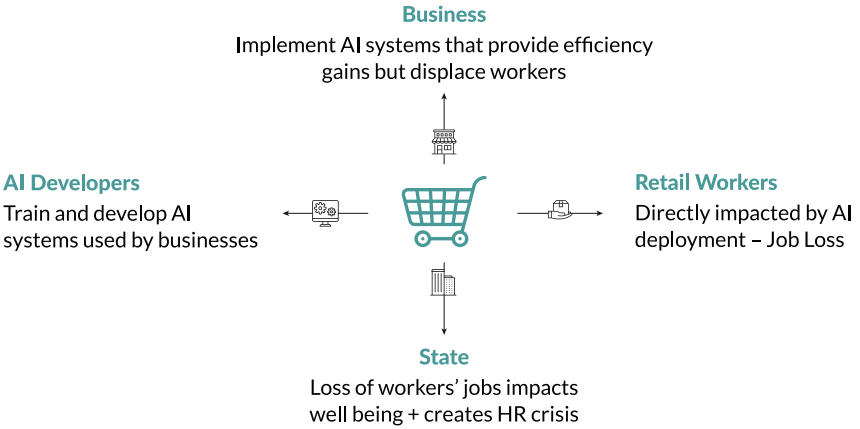


Figure 16: Stakeholder mapping for AI deployment in the retail sector

AI deployment has considerable potential to provide an increase in efficiency gains for businesses. AI systems can help businesses streamline their workforce, better predict consumer behaviour and spending patterns, and optimise inventory while reducing personnel costs. However, businesses will also have to plan strategy for handling displaced workers. For retail workers, AI deployment is a double-edged sword. On the one hand, it can make their lives easier by assisting them in tasks, and helping them streamline their workflow. On the other hand, increase in AI deployment has a proportionate effect on loss of jobs for retail workers. A 2021 survey noted that retail workers in the UK faced a 70% chance of being replaced by automation in the next few years (Electrical Direct, 2021). This has significant consequences for the State, which must balance business interests in adopting AI with the potential human rights crisis that can be created due to job displacement

and lower worker well-being. Another important stakeholder here is the AI developer. Very often, AI systems deployed by retail companies are not designed in-house, but by external service providers. While this certainly is an avenue of job creation, businesses and developers must ensure they work closely with each other to understand the full impact of the AI systems on workers, and iterate to minimise such impact.

Human Rights Risks

Human Rights Risk	Legal Frame
Loss of Jobs	• Right to Work (UDHR Art. 23; ICESCR Art. 6) • Right to standard of living (UDHR Art. 25)
Erosion of worker autonomy + risk of discrimination	• Right to enjoyment of just and favourable conditions of work (ICESCR Art. 7)

Figure 17: Human rights risks to workers as a result of AI deployment in the retail sector

Risk 1: Loss of Jobs

> ***"AI-based automation will replace all simple jobs that require basic pattern recognition in the next two decades."***
>
> - Senior executive at an AI retail solution provider (a)

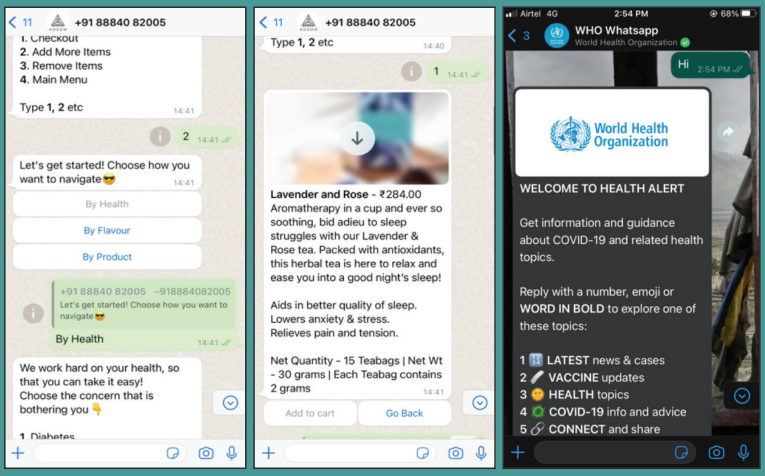
A major risk to the human rights of workers owing to AI-led automation in the retail sector is posed by the loss of jobs. Experts interviewed indicated that any job that requires basic recognition of patterns and relies on the performance of simple, repeatable tasks is very easy to automate through training AI. Review of extant literature along with conversations with experts indicates that the retail sector, especially in

India, has a very high percentage of jobs that are low-skill and based on basic pattern recognition. This places these jobs in the retail sector at a very high risk of being replaced by AI-led automation. Deployment of such automated systems leads to lower cost to the company in comparison to hiring human workers to perform the same tasks.

While it is true that AI deployment can create jobs, the skill set required for these jobs is very different from the skill set possessed by workers displaced by deployment of these AI systems. Most retailers are also averse to instituting reskilling measures as they see it as a cumbersome and possibly resource-intensive task. The resulting combination of automated systems and lack of reskilling measures crystallises the loss of jobs for human workers in the retail sector.

Box 4: Use of automated chatbots in different sectors

The most common form of customer-facing, AI-enabled automation is the use of chatbots for purchase and customer care. The images below depict the use of a chatbot through WhatsApp to facilitate purchase from a retailer.



While these chatbots pose a threat to jobs in the retail sector, the technology can have great application in other sectors, especially in public welfare. A WhatsApp chatbot has been designed by the India Literacy Project to provide career guidance to students from government schools (who are typically denied institutional access to career guidance). In March 2020, the World Health Organization (WHO) launched a chatbot on WhatsApp to provide people with the latest news and information regarding the novel coronavirus.

Risk 2: Erosion of Worker Autonomy and Risk of Discrimination

"AI-based workforce management systems require human intervention at the management level."

- Senior executive at an AI-based workforce management solution provider

Many retailers are turning to AI-trained software for workforce management. Such software forces workers to interact with systems rather than humans. The software operates on the basis of training datasets, leading to operation in largely black and white terms. In many instances, the software is trained using datasets that are skewed or biased and as a result it perpetuates these institutional biases. This can lead to discrimination against workers on multiple bases, such as gender (Dunga, 2020).

This bias is seen especially when it comes to hiring. If the data used for past hiring and promotion decisions is biased — or the algorithm is designed in a way that reflects bias — then future hiring decisions will be biased too (Kassner, 2021). For example, Amazon was forced to scrap the recruiting engine it used as it was discovered that the system gave preference to men over women. This was due to the fact that the system was trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period, when most applications were from men (Dastin, 2018).

Some experts interviewed highlighted that reporting through the means of AI-enabled software removes any scope for subjective discretion that would have been exercised in exceptional cases if the worker was reporting to a human manager. For example, a worker clocking in late owing to meeting with an accident out of their control would be excused by a manager. However, the software would only recognise that the worker had clocked in late and consequently dock/reduce pay. AI-enabled software also requires a certain level of technical knowledge on the part of the workers and in the absence of any effective training leads to erroneous capture of information regarding worker productivity, which

has resultant impacts on worker performance appraisal. Expert interviews also highlighted that the removal of humans from the decision-making process reduces the degree of accountability in the system, exposing workers to further discrimination and bias. Review of extant literature indicates that while AI-enabled workforce management software can provide significant efficiency gains for both management and workers, it is imperative that there be periodic human intervention at management level to ensure that instances of bias and discrimination are resolved and cases deserving of subjective discretion are treated accordingly. This was corroborated by the experts interviewed.

Gig work and AI algorithmic intermediation: Risks to standard of living, social security, privacy and effective remedy

Gig work involves temporary jobs, typically in the service sector, where the worker is engaged as an independent contractor or freelancer. In most cases, the allocation of tasks is mediated by a platform company. Despite still being in a nascent stage, the gig economy in India has seen rapid growth. The COVID-19 pandemic has further fuelled this growth, with numerous 'full-time workers' losing their jobs and a simultaneous increase in e-commerce during the pandemic. Studies indicate that the gig economy in India is expected to grow to USD 455 billion by 2024 (ASSOCHAM 2021), with India likely to have 350 million gig jobs by 2025 (IBEF 2021).

A key aspect of the functioning of gig work companies (on-demand platforms) is the use of algorithms to intermediate work, mainly for allocating work and determining workers' compensation. Common tasks carried out through gig work include delivery of goods, personal grooming services, maintenance services, and contract carriage.

Understanding flow of work in on-demand platforms

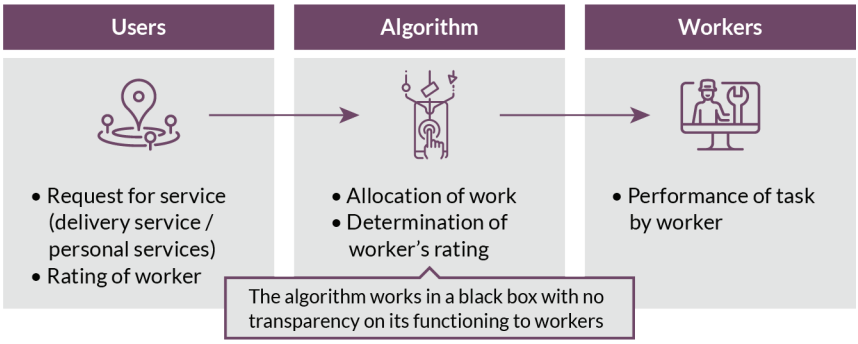


Figure 18: Flow of work in on-demand platforms

A typical online platform uses an algorithm to allocate a particular worker to complete a task logged by a user on the platform. Metrics used by on-demand platforms to evaluate worker performance are not transparent or subject to appeal. The algorithm, through the app, allocates a particular worker to complete the task. On completion, the user is asked to rate the worker on the app. The rating is not displayed to the worker and is used by the algorithm, in conjunction with numerous other factors, to calculate an aggregate rating for the worker. The rating given by the user is final and not subject to review or challenge by the worker. The determination of the worker's aggregate rating is performed by the algorithm, which is treated as confidential information and not subject to review. Expert interview analysis showed that workers are not told the precise criteria that go into the determination of their rating. This aggregate rating is also taken into account by the algorithm while allocating work to the worker.

Stakeholder mapping

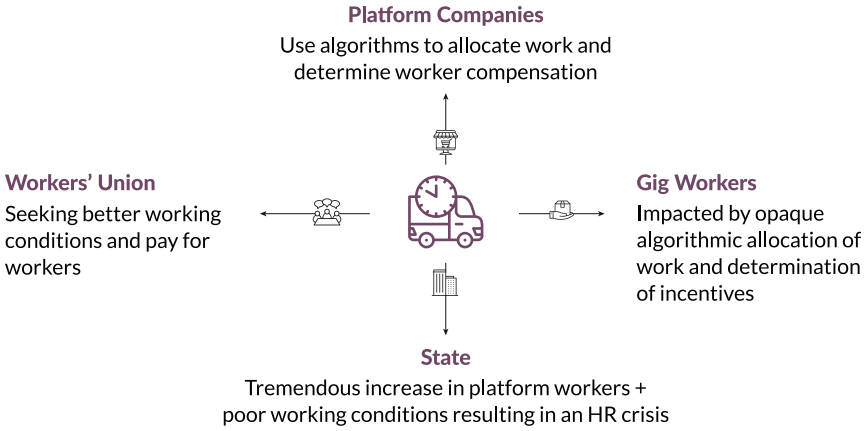


Figure 19: Key stakeholders in the gig work space

The gig economy has proven to be a massive job creator, with around 15 million Indians currently working in the gig sector. The COVID-19 pandemic has resulted in large-scale job losses in traditional sectors, and displaced workers have sought refuge in the gig sector. However, gig workers are also impacted by the opaque nature of algorithmic allocation of work and determination of incentives. Top platform companies have also come under criticism for their human rights and labour practices, which are seriously affecting the well-being of numerous workers.

The State has a dichotomous relationship with the gig work sector. While this sector has created millions of jobs, and provided a means of employment for many, especially from rural and lower educated backgrounds, the poor working conditions and labour issues that have become synonymous with major gig work companies are a major concern for the State. Regulating the gig work sector has proven to be a complex task for jurisdictions around the world, owing to the unique nature of this space.

Worker unions, which can be found in almost all sectors, have been slow to form in the gig work space. The intermediation of work through mobile apps has made it

harder for workers to unionise, and platform companies have also been reluctant to engage with unions. However, the rising demand for better working conditions and pay for platform workers has seen a rise in the number of workers joining gig worker unions. The unions are now an important stakeholder within this sector, providing a unified voice for the concerns faced by lakhs of gig workers.

Human Rights Risks

Human Rights Risk	Legal Frame
Inadequacy of Income + Poor working conditions	• Right to standard of living (UDHR Art. 25) • Right to enjoyment of just and favourable conditions of work (ICESCR Art. 7)
Worker Surveillance	• Right to Privacy (UDHR: Article 12, ICCPR: Article 17)
Absence of social security	• Right to Social Security (ICESCR Art. 9)
Risk to effective remedy and grievance redressal	• Right to effective remedy (lack of contestability) (UDHR: Article 2, ICCPR: Article 8)

Figure 20: Human Rights risks to workers as a result of algorithmic mediation of work

Risk 1: Inadequacy of income and poor working conditions

On-demand platforms use AI algorithms to determine a worker's aggregate rating. As the rating is linked to the income of the workers as well as the allocation of jobs to them, the opaqueness in the determination

of ratings has a severe detrimental impact on the rights of the workers.

While workers receive a fee for performing a job, a sizeable portion of their income depends on incentives provided by the platform. These incentives are typically linked either to the worker's aggregate rating or to the number of jobs completed within a fixed time frame. For example, a driver working for a cab hailing firm is eligible for an incentive if his rating at the end of the week is greater than 4.8/5; similarly, drivers qualify for an incentive if they complete a certain number of rides by the end of the week. Parallelly, the aggregate rating of the worker is also a determinant factor in the number of jobs he gets through the platform.

Interviews with gig workers and experts, and existing literature show that the opaqueness in the AI algorithmic determination of rating contributes to workers receiving inadequate income. Five gig workers we spoke to pointed out that often their rating would mysteriously drop just before the incentive was to be calculated. Similarly, some workers also noted that as they got closer to achieving the requisite number of jobs that would qualify them for the incentive, they would get allotted fewer and fewer jobs despite no change in rating. These experiences were corroborated by experts who either work with gig worker unions or have conducted studies on the experiences of gig workers (Gupta & Natarajan, 2019). Gig workers and experts noted that any complaints regarding such incidents are rebuffed by platform companies who point to the AI algorithm being responsible for determination of ratings and allocation of work (PUDR, 2021). Women face aggravated issues in this instance as most women doing gig work also have domestic responsibilities (Siddiqui & Zhou, 2021). As a result, they are unable to take advantage of the 'peak hour' benefits as they are occupied with household responsibilities (Kasliwal, 2020). The algorithms, experts said, do not account for women being unavailable during certain hours (Gupta & Natarajan, 2019). Companies are thus able to hide behind the garb of algorithmic determination while workers end up receiving inadequate income (Raibagi, 2021).

The lack of algorithmic transparency also forces workers to put up with very poor working conditions. As the rating by the user will determine the income they receive as well as their ability to get jobs on the platform, workers are forced to perform additional tasks

for no pay or go out of their way to satisfy the customer (Athreya, 2020). Experts interviewed confirmed that workers are also not allowed to reject more than a handful of jobs without the rejection affecting their rating. Further, in cases of time-bound tasks, gig workers we spoke to said they were forced to drive recklessly and on occasion commit traffic violations in order to ensure that their rating did not drop. This has also been corroborated by news reports, with even the police acknowledging the role that the incentives system plays in this (Prasad, 2018; Rawat, 2019).

Women, again, face heightened concerns relating to their personal safety. Women in gig work largely perform grooming and personal care services, which require them to enter private spaces, where their safety is at risk. The responsibility for their safety is left to them, and not taken up by the platform (Chitkara & Tandon, 2021).

Risk 2: Worker Surveillance

In order to be able to get jobs through on-demand platforms, workers are typically forced to constantly share their location data. With the onset of COVID-19, on-demand platforms started mandating that workers share sensitive personal health information, including body temperature, which is displayed to customers on the app. To ensure that they were wearing masks, the experts said, they were made to share photos of themselves through the app.

The worker's rating also functions as a surveillance tool (Athreya, 2020). As the rating is linked to worker actions on the app (such as how many jobs they reject, how many jobs they perform), ratings are used to keep a tight control over workers' duration of activity on the app, acceptance and cancellation rates and compliance with company policies (Newlands, 2020). The rating system therefore acts as a de facto surveillance tool (Gupta & Natarajan, 2019).

Box 5: Consequences of opaque algorithm for a gig worker

The lack of transparency of the algorithm has detrimental consequences on income, working conditions and ability to get redressal for workers.

"The incentives are important for me, because without them the income from rides alone is not enough. For the incentives, my rating is very important. If my rating at the end of the week is 4.8 or more, then I will get the incentive. But in many cases, and this has happened to other drivers also, my rating will be 4.8 or more for the whole week but one or two days before the end of the week, it will go down to 4.78 and I won't get the incentive. Initially, I would try to call the call centre and ask about it. They just say that it is determined by the app (the algorithm) and so they don't know. They say that maybe some customer gave me a bad rating, but I check with customers and request they give me five stars. Because of this, I also can't cancel more than two or three rides in one day. If I do, then my rating will automatically go down. It's very easy for the rating to go down, it goes down quickly in one or two days, but it takes some five to six days for it to go back up to a good level. If the rating goes down too much, we are just locked out of the app. Then I have to go to their central complaints centre and wait. And there is no guarantee that they will resolve it in one day. We have to hope that they will do it fast, because otherwise we can't earn anything."

Risk 3: Absence of Social Security

As highlighted earlier, gig workers are classified as independent contractors and are thus not entitled to social security protections typically afforded to employees, including health insurance, pension contribution, or paid leave. The lack of social security has a disproportionate impact on women, who typically work jobs which involve seasonal high periods. Besides, they are not eligible for maternity leave.

"I don't work for multiple platforms because, to get a decent wage, I need to qualify for the incentives, for which I need to work more for one app alone."

- Gig Worker (c)

Research based on interviews with gig workers and experts, as well as a review of literature, reveals that platform companies are able to collect vast tracts of data about workers and, using the algorithm, are able to dictate worker behaviour in a manner similar to an employer (Siddiqui & Zhou, 2021). In many cases, workers are effectively 'locked-in' to an app as, in order to be eligible for incentives, they are forced to spend most or all of their working time with a single platform company (PUDR, 2021).

Risk 4: Lack of effective remedy and grievance redressal

"Often, when we ask why the rating was lowered, they say it was because of the app and they don't have visibility into it."

- Gig worker (d)

The unaccountable nature of the algorithm results in workers having no recourse to understanding why their rating was lowered or why they are being allocated fewer jobs. The lack of a legal requirement for explainable AI worsens the plight of the workers who are left in the dark regarding their ratings.

Additionally, gig workers who were interviewed noted that the automated customer care mechanism, which is the first recourse available to workers, is ineffectual. Moreover, workers who fall below a particular rating are automatically locked out of the app and are required to travel to a central complaint redressal centre, which is typically a day-long affair with loss of pay. Some workers even reported having to visit these centres over a period of two to three days to have their account access restored. This was corroborated by experts, including union members and academic researchers.

Unexplainable AI, along with poor complaint redressal mechanisms, means that workers lack effective means of remedy and grievance redressal, which is accentuated by the primacy given by on-demand platforms to customers.

Box 6: Algorithmic mediation of work acts on top of existing social inequities to disproportionately affect women

Algorithms may be gender neutral on the face but, given India's prevailing structural inequalities, the impact of AI deployment on women is disproportionate in comparison to men. This is particularly evident in gig economy work. Most women doing on-demand work perform personal grooming and care services, which are seasonal in nature. Therefore, while there are periods where there is high demand – for example, the months of November and December, which mark the wedding season in India – they also have to endure long periods with little to no income.

Despite the nature of effective control exercised by platforms, given the classification of gig workers as independent contractors by the platforms, women are denied a minimum wage which may support them during the months when there is low demand for such services. Similarly, the lack of social security protections is heightened for women who inevitably have child bearing and raising responsibilities.

The traditional patriarchal nature of Indian society also means that women have to manage domestic responsibilities and are thus unable to spend as much time on the app as men, thereby reducing their earning window.

Finally, free mobility for women is usually an issue as many women are reliant on male members of the household to accompany them when they travel outside. As a result, women's ability to accept and carry out work is limited to when male members are also free to accompany them.

Alternatively, women are made to constantly update family members about their whereabouts, or share their live location with them, increasing the surveillance that women are subject to. This also makes grievance redressal a bigger issue for women.

The use of ineffective AI systems for grievance redressal forces workers to visit the central complaints centre for any meaningful resolution of grievances. As many women's ability to visit the central complaints centre is dependent on a male member of the family accompanying them, it makes the grievance redressal process for women gig workers complicated.

05 /

Pathways for mitigating risks

The UN Guiding Principles on Business and Human Rights constitute the world's most authoritative framework for responsible business conduct. The first part of this chapter unpacks the underlying matrix of interests for businesses to respect human rights. Then it proceeds to demonstrate how the UNGPs can serve as a framework to outline actions required of the State to protect human rights in the use of AI by businesses. Further, this chapter illustrates how the UNGPs can provide guidance to business to ensure respect of human rights for both consumers and workers.

The last section outlines the strategies for human rights risk mitigation that need to be adopted by the State and business in each sector to detect and mitigate every risk identified. Pathways for mitigating risks are based on the UNGPs' three-pillar framework of 'Protect, Respect and Remedy' that outlines roles for the State and business. Under the UNGPs, the State has a duty to protect human rights (Pillar 1) and businesses have a responsibility to respect human rights (Pillar 2). Access to remedy (Pillar 3) ensures effective redressal for victims of human rights abuses.

Pushing the business case

There is a matrix of interests for businesses to respect human rights. Each sector has a unique set of incentives to align business interests with the UNGPs' Business and Human Rights framing.

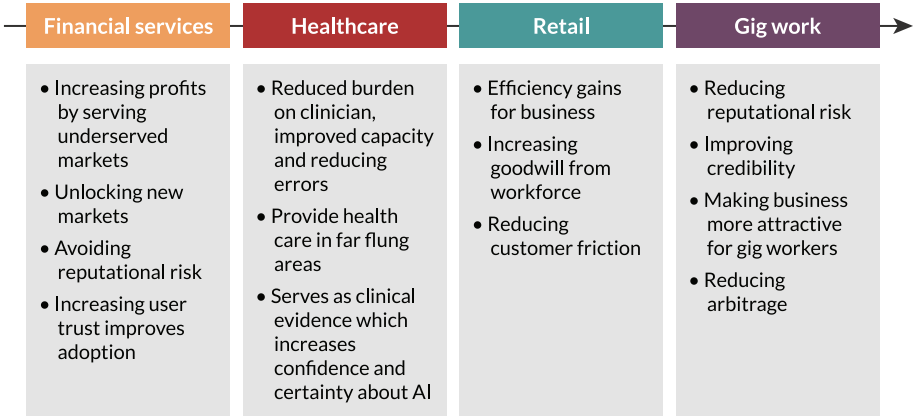


Figure 21: Varying interests of businesses by sector

Financial services

Businesses increase profits by serving under-served markets which is the primary business model for digital lenders. Respecting human rights not only helps businesses unlock new market segments previously excluded due to a lack of credit history, it also expands consumer base by attracting consumers with credit history to avail of digital lending services, drawing them away from traditional modes of lending by increasing user trust. The reputational risk for legitimate lenders is high, given existing circumstances where there is a slew of predatory lenders exploiting consumers, threatening adoption of services. Legitimate lenders must, thus, proactively respect human rights in order to clearly distinguish themselves from predatory lenders who have no incentive to respect human rights.

Healthcare

The efficiency of healthcare systems is enhanced as the burden on clinicians is reduced. With clinicians having more time, they are better able to tend to patients due to optimised capacity and reduction in errors. With 70% of our healthcare infrastructure concentrated in cities, catering to only 30% of the country's population, AI technology can potentially solve for the gap in supply and demand of healthcare services in remote and rural areas (Research and Markets, 2019). There is an increased ability to provide healthcare in far-flung areas by providing capacity to local doctors to triage. Clinical evidence is required to have confidence and certainty regarding AI and is critical to adoption of AI by doctors and hospitals in healthcare. As AI systems align with human rights, the likelihood of its adoption increases in the sector.

Retail

Respecting human rights in the context of AI deployment for businesses in the retail sector can have multifold benefits. The increase in AI adoption will demand a different set of technical and personnel skills from the workforce, and while it is possible for businesses to hire from outside it is far more efficient for them to reskill or upskill existing workforces and

equip them with the necessary tools to perform these tasks. In addition to direct benefits in terms of payroll, reskilling workers will also attract goodwill from both consumers and workers. This makes the business a more attractive place to work for existing and prospective workers, while consumers are more likely to interact with a business that shows concern for its existing workforce.

By reskilling existing workers, businesses also ensure that they retain institutional knowledge within the firm, and reduce intangible costs involved in onboarding new employees and acquainting them with the culture and ethos of the business. Overall, respecting human rights can help businesses increase profitability and create a more motivated and driven workforce.

Gig work

Respecting human rights reduces the reputational risk and improves credibility of businesses. Further, businesses are as good as the services they provide. In gig work, the apps are as efficient as the number of platform workers who are available to take up the tasks. The competition among these apps is extremely high as search costs to avail of a service are nearly equal with all apps being equally easily accessible to consumers. Respecting human rights makes businesses attract platform workers and increases retention. Furthermore, it also reduces arbitrage.

Roles for each stakeholder across sectors

The State and businesses share responsibility to work towards a practical and workable approach of deploying AI in business operations that are aligned with the UNGP framework. The measures outlined in Figure 22 must be implemented by the State and businesses.

State	Businesses
Create incentive for businesses to adopt the HR framing through regulation	Need to pay attention to existing correlation of business incentives with human rights; formulate internal policies that enable respecting human rights
Support businesses by establishing capacity building measures	Focus on making explainable AI
Ensure enforceability of existing norms and regulations; consider extending applicability of laws to AI technology, wherever possible	Maintain a minimum stipulation of human intervention and oversight in AI deployment across sectors

Figure 22: Broad measures to be implemented by the state and businesses

State

Create incentives for businesses to respect human rights through regulation

The State must create incentives by enforcing laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically assess the adequacy of such laws and address any gaps as stipulated under Principle 3 (a) of the UNGPs on Business and Human Rights.

There are two primary barriers to respecting human rights in business operations – lack of business willingness and lack of ability (technical, financial or infrastructural) to detect and mitigate human rights risk. Where profitability and human rights are often perceived as poles apart, businesses hesitate to respect

human rights as they fail to assess the business case for doing so. The State has been recognised as a stakeholder that can create incentives through regulation which directly pushes businesses to respect human rights.

For instance, mandating regulatory approvals for AI technology application in the healthcare sector would push businesses to check for biases in their technology. There is notable business unwillingness to check for such biases in the absence of regulation. In the financial services sector, the State can create competition regarding privacy and data by setting up a framework for consumer rights and penalising businesses for data breaches. In retail, the State can pass legislation requiring companies to mandatorily provide reskilling courses to employees whose jobs are affected by the adoption of AI automation. In gig work, robust regulation on having a fair contract, as well as a statutory allowance for social security and minimum wages can ensure that gig workers have fair pay and social security protection.

Support businesses by establishing capacity building measures

The Government of India has a duty to ensure policy coherence by establishing capacity building measures to support businesses, as stipulated under Principle 8 of the UNGPs. Principle 8 enjoins that government departments, agencies and other State institutions that shape business practices be aware of and observe the state's human rights obligations when fulfilling their respective mandates, including by providing relevant information, training and support. Even if businesses are aware of the human rights risks and actively seek to detect and mitigate them, they are unable to do so effectively, given a lack of technical expertise, finances and infrastructure. Thus, the role of the government should not be limited to regulation but also include capacity building measures to ensure businesses are apprised of what must be done to mitigate these risks. The government must provide effective guidance to business enterprises on how to respect human rights in deployment of AI.

For instance, India as a low and middle income country does face the pressing issue of lack of good quality data – data which is error-free, complete and diverse. Creating datasets that are non-biased and representative

in a country like India which is vast, segregated and diverse is a herculean task for Indian businesses currently in nascent stages with limited access to finance and infrastructure. The government plays a key role in enabling availability of resources such as unbiased and representative data, fundamental to risk detection and mitigation, given that it benefits from risk-free AI deployment through achievement of the broader goals of economic equality, increased access to quality healthcare and financial inclusion.

The State benefits from ensuring that workers are employed and adequately compensated. Setting up skilling courses for workers or government contributions to social security funds can mitigate the risks of unemployment and low quality of life as a result of inadequate income. The role of the State should thus, in addition to regulation, also include capacity building measures to overcome technical inability of start-ups to mitigate risks in governance practices.

Ensure enforceability of existing norms and regulations; consider extending applicability of laws to AI technology, wherever possible

Lawmaking is a slow process requiring in-depth understanding of the technology. AI is constantly changing and the law fails to keep up with evolving technology. However, the impact on the human rights of citizenry is real and on-going, and, in fact, aggravated for vulnerable populations.

Under these circumstances, the State must immediately take up measures to mitigate the impact to the best of its ability. It was highlighted by experts across sectors that there is an immediate need for the State to bolster the current regulatory framework to accommodate emerging technologies and mitigate their risks to human rights. Under Principle 3 (c) of the UNGPs, the State must "ensure that other laws and policies governing the creation and ongoing operation of business enterprises do not constrain but enable business respect for human rights".

For instance, in the financial services sector, RBI norms backing the right to know the reason for credit denial are applicable only to formal lending institutions such as banks. It must be made applicable to AI-based credit lending as well. In gig work, the

Code of Social Security, 2020, is a good framework stipulating worker rights. However, the State must strive to operationalise this framework of rights for AI-intermediated gig workers. Across sectors, experts believe that in the absence of privacy legislation, applicability of existing legal principles can be extended to automated decision-making.

For instance, the principle of 'due process' ensures that decisions affecting individuals are procedurally safeguarded against arbitrariness. Procedural safeguards include the right to know the reason for the decision, the right to know the information based on which the decision was made and the right to contest the decision.

Businesses

Need to pay attention to existing correlation of business incentives with human rights; formulate internal policies that enable respecting of human rights

This report unpacks business incentives to respect human rights. There is a need for businesses to pay attention to the evidence that suggests that profits do follow when businesses respond to human rights risks. As reiterated by experts, businesses must understand the basic rule of long-term sustainability – that responding to consumer needs is essential. Though the short-term costs are high, which is a factor deterring businesses from respecting human rights, the long-term benefits of credibility and profitability are a given. Businesses must adopt internal policies that enable them to respect human rights. For instance, businesses must adopt a human rights policy which also governs AI deployment in their operations. Under Principle 16 of the UNGPs, businesses that appreciate the risks they pose to consumers and workers can formulate a public commitment in the form of corporate policy to ensure all employees, including managers, respect human rights in deployment of AI.

Businesses should deploy personnel from diverse backgrounds (caste, ethnicity, religion and gender) with educational qualifications not limited to technical expertise in AI technology but also social sciences in their AI development teams. In this way businesses can begin to respect

human rights, which gets reflected in their hiring procedures, as stipulated under Principle 16(e) of the UNGPs.

The adoption of the Risk Assessment Toolkit, attached as Annexure B, would be the first step in conducting a Human Rights Due Diligence (HRDD), as prescribed in Principle 17 of the UNGPs.

Further, businesses must collaborate with other relevant stakeholders and consult with other potentially affected groups, as stipulated under Principle 18(b) of the UNGPs. For instance, in the financial services sector, membership of industry associations such as the Digital Lending Association of India allows members to collaborate and share technical knowledge on how to detect and mitigate AI bias, which is particularly useful for small start-ups who lack the technical know-how. In the healthcare sector, clinicians should be made a part of the AI development process to help detect inherent biases in the technology.

Focus on making explainable AI

Though the State is responsible for creating an environment for businesses to thrive and for guiding business policies and practices with respect to AI, it cannot directly interfere with the manner in which the technology works. Businesses are directly involved in the deployment of AI and are in a better position to modify the technology to mitigate human rights risks stemming from its deployment.

Businesses can identify and articulate the risks by conducting HRDD, as outlined in Principle 17 of the UNGPs. Following a mapping of the risks, businesses should prioritise actions in consultation with stakeholders, and integrate risk mitigation strategies into their business processes and across internal functions, as outlined in Principle 19. For instance, experts noted that across sectors businesses should focus more on their strengths of technical expertise and endeavour to make AI more explainable and transparent for its end users – consumers and workers.

Maintain a minimum stipulation of human intervention and oversight in AI deployment across sectors

Despite advanced automation in AI, decision-making by it in critical processes, operations or workflows should be monitored by human intelligence. This is the best approach to ensure fairness in decision-making. Under Principle 19 (a) (ii) of the UNGPs, internal decision-making and oversight processes are effective responses to mitigate human rights risks.

Given that the utility of AI is decision-making, it may seem redundant to necessitate human intervention as leading to duplication of efforts and wastage of resources. However, all decisions cannot be left to the discretion of AI, especially now that evidence exists of its potential impact on populations due to flawed decision-making and the risks it poses to citizenry. Thus, a proposed middle ground solution is for businesses to differentiate between critical and non-critical processes, based on the impact of decisions for the business and for the party it relates to, and necessitate human intervention only for critical decisions.

For instance, in the healthcare insurance sector, the decision regarding denial or granting of coverage is critical as it impacts consumers' ability to access healthcare, in comparison to usage of AI for regular automation and simplification of standard business processes. In the financial services sector, AI deployed in consumer facing apps can refer serious issues to professional medical practitioners.

Sector-wise risk mitigation strategies

Financial Services

Risk mitigation strategies, according to the UNGPs' 'Protect, Respect and Remedy' framework, can broadly be summarised as:

- The State should focus on enforcing of consumer rights, penalising lenders for breach of their fiduciary duty, and strengthen capacity building measures for businesses.
- Business should create explainable AI, apply AI responsibly and collaborate with industry members.
- Remedy frameworks should be consumer-centric, focussing on spreading awareness and facilitating legal redressal.

Pillar 1:

The State must set up the regulatory framework to create an environment that pushes competition in safeguarding privacy

The State must create competition in safeguarding privacy from both ends – supply and demand. On the demand side, enforceability of consumer rights is key. Enforcement of the PDP Bill, 2019, sets the framework for consumer rights and it aligns with the UNGPs (Principle 3 (a)) that stipulate the duty of the State to enforce laws. However, under Section 14 of the PDP Bill, personal data can be processed without obtaining consent for reasonable purposes which include credit scoring. It is thus suggested that prior and explicit informed consent be obtained from consumers, as reiterated in the RBI Report of the Working Group on digital lending.

The State must also take up measures that increase consumer awareness of the value of their data. The trade-off propels businesses' adherence to the principle of minimum data collection. For instance, experts

noted that the State should mandate the publication of loan disbursement rates. Consumers can assess the value of their data by comparing acceptance rates. A consumer would prefer to share his data with a player with a higher acceptance rate. The ability of consumers to assess the value of their data plays out more easily in the digital lending sector, given that the consideration is monetary as against other sectors where data is provided in exchange for monetarily free services, as in social media.

On the supply side, any breach in regulation will lead to a penalty. The PDP Bill relies on the concept of data fiduciaries which places the responsibility on the provider to act in the interests of the consumer. Given that Indian consumers do not provide informed consent, the placing of a fiduciary duty on providers helps to reduce the burden of providing informed consent.

In the digital lending sector, the State should enforce consumers' right to know the reason for credit denial, making it the duty of businesses to ensure AI is explainable to consumers. Such regulation incentivises businesses to document credit denial and detect biases. Experts noted that currently, in India, most businesses prefer outsourcing explainable AI. Mandating explainable AI is a move in the right direction, bolstering grievance redressal and ensuring business accountability for AI-based decisions. The right to know the reason for credit denial is afforded to consumers of formal lending institutions such as banks under the RBI norms[6]. It must be made applicable to consumers of AI-based lending also. Extending the application of existing laws or certain principles can help fill the regulatory void, as stipulated under Principle 3 (c) of the UNGPs. This has been reiterated in the RBI Report of the Working Group on digital ending which recommends the documentation of algorithmic features used in digital lending to further transparency and enable explainable decisions.

Another form of positive reinforcement would be to directly incentivise businesses when they adhere to privacy principles according to objective norms set by the State. For instance, standardised consent makes the marketplace more competitive.

The enforcement of the PDP Bill will

[6] Reserve Bank of India, Master Circular on Loans and Advances – Statutory and Other Restrictions, July 1, 2015. Available at: https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9902

also afford consumers the right to access, rectify and update their data which helps to prevent inaccuracies in determination of creditworthiness. AI audits by the State will help in detection of biases and is an important measure supporting businesses in detecting and mitigating biases, as reiterated in Principle 8 of the UNGPs.

Pillar 2:

Business should focus on creating pathways for informed consent

The focal point of data privacy issues is consent. However, the question now is not about consent but about creating pathways for informed consent. Business policy must reflect intention to create meaningful pathways for informed consent. Principle 16 (e) of the UNGPs enjoins that operational policies and procedures of businesses must reflect their commitment to respect human rights. As reiterated across expert interviews, the service provider bears responsibility for ensuring informed consent and merely seeking consent through the 'notice and consent' mechanism is not the solution for several reasons. First, several behaviour biases operate, incapacitating consumers to understand that a certain provider is not right for them, in addition to their inability to read and understand the clauses. For instance, present bias occurs when consumers are ignorant of future harm stemming from unmindful sharing of data for immediate gains such as loans, and cognitive overload occurs due to legally complex and lengthy privacy policies (CSBC and Busara Research, 2020). Second, all service providers have the same standard contract template of consent, providing no competition or choice for consumers to overcome their flaws.

Consenting needs to be improved. It is not a sufficient safeguard for data protection, but a very necessary one. It provides the first occasion to express autonomy, widely accepted throughout the human rights and legal regime circles. For instance, research in India indicates that consumers need to be nudged to be more privacy conscious. Indian consumers respond well to hard nudges such as the cool-down period (mandating users stay on the privacy policy page for a fixed period of time) and high star rating (indicator of the quality of privacy policy) which need to be integrated into the product design (CSBC and Busara Research, 2020). Businesses benefit as these nudges

increase trust and data sharing amongst consumers.

Consent must further be bolstered by technological solutions. Technology needs to be regulated by technology. There is a need to move beyond general technological solutions such as privacy by design and deploy specific technological solutions such as AI auditing. Internal AI audits conducted by businesses help to detect and mitigate biases in the AI technology, which is in accordance with the UNGPs' Principle 17 that suggests businesses conduct HRDD to identify, prevent and mitigate human rights risks.

The primary issue is not the lack of technological solutions but the cost which makes them unimplementable. The focus is thus on making technology cost-effective and implementable. Experts noted that efforts by businesses need to be made collectively. Industry leaders can pave the way by sharing insights on how technology can be utilised to increase privacy and mitigate biases. This reduces the search cost of finding the most appropriate solution. Businesses do have an incentive to participate in such knowledge sharing as it creates an atmosphere of trust amongst consumers, benefitting all players in the market.

Businesses can compete with one another regarding privacy by making AI explainable. Experts noted that businesses should focus on their key strengths to improve the AI technology, that is, making it as explainable as possible. This means that they should be in a position to understand how the technology works and also make it decipherable to lay consumers. This measure helps businesses adhere to Principles 17 and 19 of the UNGPs (articulating the risks they pose by conducting an HRDD (Principle 17) and subsequently integrating the risk mitigation strategy by making AI more explainable (Principle 19)).

In order to mitigate algorithmic biases in AI-based credit scoring, businesses need to be more mindful in determining the relevancy of the metrics. Metrics need to be made relevant to the populations being catered to and should, as reasonably as possible, represent the creditworthiness of the consumers accurately. Businesses should focus on hiring persons with the relevant skills and qualifications such as social scientists who understand population dynamics and can help prevent biases from creeping into the technology.

Risk 1: Risk to privacy

Protect

State

- Regulate, with a focus on:
  - *Setting up the framework of consumer rights (e.g. enforce consumers' right to prior and explicit informed consent)*
  - *Creating incentives to increase competition regarding privacy amongst businesses (e.g. mandate publication of loan disbursement rates)*
- Enforce Personal Data Protection Bill, 2019
- Enforce consumers' right to know reason for credit denial to ensure that businesses are made accountable for their data collection practices.

Respect

Business

- Recognise that notice and consent may not be an adequate tool in data protection
- Deploy specific technological tools and solutions that help consumers give informed consent (e.g. cool-down period, high star rating, etc)
- Collaborate with other industry members to make technological solutions more implementable, given that they are expensive to deploy.

Remedy

State

- Set up remediation channels through legislation
- Mandate that businesses set up grievance redressal portals.

Business

- Set up an in-house grievance redressal mechanism as the first point of escalation (e.g. operationalise chatbots on consumer facing digital lending apps)
- Lay out various options for remedy and redressal available (judicial and non-judicial) for consumers to resort to in the event they are not satisfied with the in-house redressal.

Remedy

Civil Society and Consumer Groups

- Focus on demand side by propelling competition regarding privacy through consumer awareness of rights
- Focus on supply side by propelling competition regarding privacy by highlighting research that displays the relationship between human rights and profitability
- Industry bodies can highlight to businesses the incentives for respecting human rights.

Risk 2: Risk to financial access and well-being

Protect

State

- Regulate to overcome barriers of lack of willingness by businesses:
  - *Stipulate a broad law for digital lending which encompasses AI-based credit scoring*
  - *Conduct AI audits to detect bias in output based on normative standards*
- Establish regulatory sandboxes to overcome barriers of inability to test the reasonableness of metrics
- Mandate publication of loan disbursement rates. Information should divulge details about denial of loans, facilitating comparison of lenders and enabling consumers to exercise their right to choose
- Support businesses in:
  - *Raising awareness of bias*
  - *Creating systems where technical capabilities can be shared.*

Respect

Business

- Initiate leadership and efforts: Industry giants can benefit by providing best practices to detect and mitigate bias by setting the rules
- Deploy low-cost measures to detect and mitigate bias using NLP to process contracts.
- Revise metrics when catering to diverse populations; tailoring the metrics according to the specifics of the population (measures can include employing social scientists who better understand population dynamics)
- Document all processes involved in algorithmic deployment to help detect the existence of bias and track how it could have crept into the model. For instance, businesses should document which metrics were considered as relevant and the underlying reason, the sources of their input data, and the reasons for denial of loan.

Remedy

State

- Establish a separate channel for remediation where grievances with respect to digital lending can be raised. Such a channel can comprise members well versed with digital lending and the AI technology as well.

Business

- Set up in-house grievance redressal mechanism as the first point of escalation (e.g. operationalise chatbots on consumer facing digital lending apps)
- Lay out various options for remedy and redressal available (judicial and non-judicial) for consumers to resort to in the event they are not satisfied with the in-house redressal.

Civil Society and Consumer Groups

- Push the business case that diversity is linked to profitability.

Risk 3: Risk to life, dignity and safety

Protect	**State** • Regulate to keep a check on and penalise predatory digital lenders • Adopt similar strategies to mitigate the risk to financial access and well-being, given that financial harms can pose a threat to life, dignity and safety.
Respect	**Business** • Actively seek to distinguish themselves from predatory lenders (e.g. publication in the newspapers to make consumers aware) and take up action against predatory lenders legally (e.g. non-predatory lenders should regularly conduct due diligence for copyright infringement and sue predatory lenders for copyright infringement of their domain names) • Adopt strategies to mitigate the risk to financial access and well-being, given that financial harms can pose a threat to life, dignity and safety.
Remedy	**State** Adopt strategies to mitigate the risk to financial access and well-being, given that financial harms can pose a threat to life, dignity and safety. **Business** Adopt strategies to mitigate the risk to financial access and well-being, given that financial harms can pose a threat to life, dignity and safety. **Civil Society and Consumer Groups** • Create awareness amongst consumers on the existence of predatory lenders • Create awareness amongst consumers on the measures that lenders can legally resort to, to ensure repayment of loans • Assist consumers in accessing remediation/feedback frameworks in the event of harassment.

Risk 4: Risk to effective remedy and grievance redressal

Protect

State

- Enforce right to know reason for denial of credit by digital lenders either by:
  - *Stipulating a new law for digital lending which encompasses AI-based credit scoring*
  - *Or, extending the applicability of existing RBI norms (currently applicable only to banks) mandating the right to know reason for credit denial.*

Respect

Business

- Maximise efforts to develop AI in-house as it makes AI explainable.
- Outsource explainable AI to increase accountability to customers.
- Focus efforts on R&D to make AI explainable.

Remedy

State

- Strengthen IP protection in India in AI to make AI explainable to the regulator.

Business

- Set up in-house grievance redressal mechanism as the first point of escalation. For instance, operationalise chatbots on consumer facing digital lending apps
- Provide reason for denial of credit in simplified language, easily decipherable by consumers
- Provide opportunity to rectify data of consumers if consumers identify that loan has been denied based on inaccurate data
- Document all reasons for loan denial and subsequent objections raised by consumers against algorithmic decisions as they will help to detect biases if loans are consistently denied to persons belonging to a particular group
- Lay out various options for remedy and redressal available (judicial and non-judicial) for consumers to resort to in the event they are not satisfied with the in-house redressal.

Risk mitigation strategies, according to the UNGPs' 'Protect, Respect and Remedy' framework, can broadly be summarised as follows:

- The State should strengthen regulation by stipulating liability and accountability regimes.
- Business should focus on clinician understanding of AI and making AI explainable.
- Remedy frameworks should be patient-centric by creating feedback loops, making patients aware of their rights and facilitating understanding of product features and utility.

Pillar 1:

The State must clarify liability and accountability mechanisms

Liability and accountability mechanisms are complex due to AI involvement in the caregiving pathway. The absence of a structured and well-defined liability and accountability regime directly affects consumer trust in the utility of AI. It is thus the primary duty of the State to stipulate frameworks of accountability defining the role, responsibility and liability of various actors involved in the caregiving pathway where AI is involved, as reiterated in Principle 3 (a) of the UNGPs. A framework of liability and accountability has been elaborated in the following paragraphs.

Patient trust in AI technology is directly proportional to the autonomy retained by the clinician in the caregiving pathway. Studies indicate that patients view the clinician as the primary caregiver bearing responsibility and thus, they must retain the final discretion with respect to patient care (Richardson et al., 2021; Verghese et al., 2018; Johnston, 2018). As further reiterated by the experts interviewed, AI is a tool that makes a clinician super intelligent, not one that replaces the clinician.

The clinician must still remain at the centre of the caregiving pathway, bearing the liability and responsibility for patient care.

However, they must document every decision where an interaction between the AI and patient took place, providing the reason as to why they relied on or deviated from the decision (Deloitte Insights, 2019). The process ensures that human judgement is applied at all stages and serves as evidence that the clinician was not in breach of their duty of care, in the event a case of medical negligence is made out against the clinician.

For the clinician to be equipped with a reasoned decision, the State must make businesses dutybound to provide an explanation of the AI working. Communication protocols must be established which fulfil minimum standards of detail, equivalent to clinician to clinician hand-off. Businesses can create mediums to educate clinicians on the function, maintenance and safety of AI which are understandable to the layman (Bitterman et al., 2020). The explanation should not be technical and complex so as to overburden the clinician. The clinician should have an idea of the populations it can be deployed on, any other product limitations, and a basic idea to understand how the decision was arrived at (key medical indicators that were relied on).

Such documentation will also give clinicians insights on the efficacy of the AI technology and push businesses to check for biases in their technology. For instance, let us take a case where the clinician relies on the AI technology based on a well-reasoned judgement but the result is not desirable. In such a case, the clinician as the primary decision-taker will not be liable as it was a well-reasoned judgement. However, the clinician will be nudged to reassess the efficacy and contemplate if the AI technology should continue to be deployed. AI developers will thus be compelled to check and mitigate biases in their model.

Liability for medical negligence cannot be placed on AI developers. A preventive method is preferred where the State through regulatory approvals permits only good quality (unbiased and accurate) AI technology to be deployed. Further, approvals will have to be sought periodically to ensure that the technology doesn't become obsolete with changing demographics. These approvals must

be based on AI audits conducted by the State, and help businesses to detect and mitigate biases, as stipulated under Principle 8 of the UNGPs. Principle 8 suggests that the GoI provide relevant information and support to businesses to detect and mitigate human rights risks. One expert noted the different kinds of AI audits that could be conducted – publication of queries to databases (data collected must be reasonably linked to the purpose of collection) and black box audits (comparison of input algorithm to the resulting output to ensure that the AI is working in the manner intended to work) (Matthan, 2017).

The State must enforce the PDP Bill, 2019, as it is a more comprehensive piece of legislation on data protection, stipulating a framework of consumer rights and remedies (compensation) and penalties for data breach. The State, in the absence of data protection legislation, must extend the applicability of the Electronic Health Records Standards, 2016, that prescribe privacy and security standards, as enjoined under Principle 3 (c) of the UNGPs.

Pillar 2:

Businesses must focus on making AI explainable

Transparency is foundational to the adoption of AI in healthcare. Transparency must exist at multiple levels – at development of the model, at point of care and at prediction level (McCradden et al., 2020).

The need for AI scrutiny is accentuated in the healthcare sector given the manner in which hospitals operate (Lynn, 2019). The clinician cannot be expected to wait to evaluate the accuracy of AI decisions. Time is an important factor in healthcare service and the clinician must be certain of the impact of the caregiving pathway. Where AI is entrusted with decision-making, it is reasonable to expect accountability. Businesses, thus, must focus their efforts on making the technology more explainable. This falls within their responsibility, as outlined in Principle 17 of the UNGPs that suggest businesses conduct an HRDD and integrate risk mitigation strategies as under Principle 19.

Transparent model development by healthcare businesses prevents the risk of bias by enabling clinicians to determine applicability of the

algorithm to the population. Declaring limitations of the algorithm mitigates the risk of bias as well as preventing it, serving as an effective remedial tool. It has been indicated that an algorithm is of utility in a specific context despite existence of a bias, provided its limitations and usage are properly disclosed and documented (Fletcher et al., 2021). Businesses resorting to this measure fulfil their responsibility of incorporating human rights in their internal policy and practices, as under Principle 16 (a) and (e) of the UNGPs.

Further, experts reiterated that since information asymmetry in healthcare is inherently skewed, with clinicians having greater insights and understanding of the patient's health, businesses should direct efforts towards improving clinician understanding of AI which is more effective than focussing on patient understanding of AI, given that clinicians are the experts who direct decision-making and the community is smaller in number. Where the clinician has clarity about the working of AI, patient trust is invariably established.

The clinician can initiate transparency acting as a mediator between the AI and the patient, facilitating explainable AI, which is critical to patient autonomy (Richardson et al., 2021). Communication with patients can be structured on choice architecture frameworks which strengthen patient autonomy (Deloitte Insights, 2019). Choice architecture frameworks influence decisions without affecting autonomy. For instance, each decision predicted will correspond to a risk score. In this way, a conclusive decision is not imparted but corresponding risk scores will influence the patient to adopt measures that are least risky.

Businesses should conduct AI audits as they build transparency at the prediction level, helping businesses to fulfil their responsibility under Principle 19 of the UNGPs that urges businesses integrate findings from impact assessments (McCradden et al., 2020). They ensure oversight over AI, help in evidence-based detection of bias and its impact on vulnerable populations, enabling interventions (Gianfrancesco et al., 2018). In the healthcare sector, certain biases cannot and should not be ignored in the development of AI given that genetic differences exist across races and ethnicities which influence the prevalence of a particular disease. In such cases, sometimes the AI model works well for one group (high

accuracy) but not for another group (low accuracy). The business should consider developing a separate model for the latter group and continue to deploy the model with an indication of its ability to work well on only certain groups (Fletcher et al., 2021).

Businesses can categorise operations as critical and non-critical and must retain oversight by human experts in critical care processes and not replace with AI (Lynn, 2019). For instance, in consumer facing apps, businesses should develop AI such that it suggests intervention by a medical healthcare professional when it is of the opinion that the problem is beyond its expertise. A mental health app in India escalates issues of serious concern to medical health professionals (Paul et al., 2018). This way, businesses adhere to Principle 19 (a) (ii) of the UNGPs that stipulates that oversight processes are impactful measures to mitigate human rights risks.

Businesses must focus on enhancing privacy and adhere to principles of minimum data collection. This may prove particularly useful for businesses such as consumer facing apps which can leverage privacy. For instance, in India mental health is still stigmatised and people are not open in talking about it. One such mental health app adopted a privacy by design approach which does not even require personal details to be filled in at the time of onboarding (Paul et al., 2018). This helped the firm to build trust and acquire more users.

Risk 1: Likelihood of bias and discrimination

Protect

State

- Establish regulatory approvals based on AI audits by measuring the algorithm based on the normative stipulation (e.g. database query audit and black box audit)
- Conduct periodic assessments of the AI as the algorithm needs to be tested against changing population demographics
- Initiate capacity building efforts for businesses by providing necessary assistance to strengthen their ability to detect and mitigate human rights risks (e.g. create publicly available datasets for those start-ups that face hurdles in accessing health data).

Respect

Business

- Focus on improving the input data. This measure should be treated as just another business constraint that can be overcome with technical advancement
- Ensure that data is correct and free from tampering
- Deploy persons from diverse backgrounds in the development team, and also include clinicians from diverse backgrounds in the data gathering process
- Work with clinicians at the AI development stage to help detect potential sources of bias
- Continue the R&D phase until the scale-up phase by training and retraining the algorithm, ensuring applicability across geographies
- Construct a separate model where the results of accuracy are low for a particular group.

Remedy

State

- Regulate AI governance by understanding its limitations and providing means to access information for consumers. For instance, measures could include mandatory publication of AI usage.

Business

- Represent product as it is and mention the product limitations.

Risk 2: Loss of individual autonomy (patient and doctor)

Protect

State

- Stipulate liability and accountability frameworks for AI usage where the clinician is the primary decision-maker and the AI is a supporting tool
- Facilitate trust amongst clinicians to increase adoption of AI technology (e.g. establish regulatory sandboxes and conduct AI audits incentivising businesses to check their algorithms for biases and inaccuracies)
- Mandate hospitals to inform patients about AI usage given that AI is distinguished from other technologies
- Enforce clinicians' right to explainable AI. The explanation should not be technical and complex and should provide information on the populations it can be deployed on, any other product limitations, and key medical indicators that were relied upon (i.e., how the decision was arrived at)
- Mandate reasoned documentation of decisions taken by clinicians in both cases – reliance on AI decision or deviation from it.

Respect

Business

- Build on clinician understanding of AI technology to increase trust and adoption; easier to target clinicians than patients.
- Develop mechanisms in AI deployment that allow interventions by clinicians (e.g. in consumer facing apps, businesses should develop AI in a way so that it suggests intervention by a medical healthcare professional when it is of the opinion that the problem is beyond its expertise)
- Create feedback loops from patients by developing new protocols around usage of AI. These protocols create avenues for patients to share their concerns about the AI technology used in their caregiving pathways.

Remedy

State

- Mandate publication of AI usage by hospitals as access to remedy is dependent on the information consumers have. If patients are not even aware of AI usage by hospitals, they cannot raise a concern.

Business

- Create patient feedback loops.

Civil Society and Consumer Groups

- Create awareness amongst businesses of human rights risks
- Focus on clinician understanding of AI
- Assist patients in accessing remediation/feedback frameworks.

Risk 3: Loss of data privacy

Protect

State

- Stipulate basic regulatory framework, for instance, the pending Personal Data Protection Bill, 2019, will be the guiding force. It is a comprehensive piece of legislation on data protection stipulating a framework of consumer rights and remedies (compensation) and penalties for data breach
- Extend the applicability of the Electronic Health Records Standards, 2016, that prescribe privacy and security standards, in the absence of data protection legislation
- Mandate consent frameworks for data collection in AI in healthcare.

Respect

Business

- Duty of healthcare providers to inform patients of AI usage
- Simplify data collection, storage and usage practices and processes for customers.
- Adopt privacy by design approach. This is particularly relevant for consumer facing apps, which must collect minimum personal data and anonymise data, wherever reasonably possible.

Remedy

State

- Set up remediation channels under legislation
- Mandate that businesses set up grievance redressal portals.

Business

- Set up in-house grievance redressal mechanisms as the first point of escalation. For instance, operationalise chatbots on consumer facing healthcare apps
- Lay out various options for remedy and redressal available (judicial and non-judicial) for consumers to resort to in the event they are not satisfied with the in-house redressal.

Civil Society and Consumer Groups

- Create awareness amongst consumers on data rights
- Assist patients in accessing remediation/feedback frameworks in the event of breach of their privacy.

Retail

Risk mitigation strategies, according to the UNGPs' 'Protect, Respect and Remedy' framework, can broadly be summarised as:

- The State should focus on capacity building measures for workers at risk of displacement and mandate effective human intervention in AI deployment.
- Business should focus on means of upskilling existing workers, and also ensure periodic oversight of the functioning of AI systems.
- Remedy frameworks should be worker-centric, focussing on welfare measures for displaced workers and adequate grievance redressal mechanisms for any human rights abuse.

Pillar 1:

The State must focus on capacity building measures

Experts were emphatic that AI-enabled automation will replace most low-skill jobs in the coming years. This has the potential to create an unemployment crisis through mass displacement of workers. In accordance with Principle 1 of the UNGPs, the State must take appropriate steps to prevent and redress human rights abuse through effective policies and regulations. In this context, the State can focus on working with businesses and experts to identify jobs which are most vulnerable to replacement by automation, and institute capacity building/reskilling measures for workers performing such jobs. AI deployment is also expected to create millions of jobs (World Economic Forum 2020). However, these jobs will require skill sets different to those possessed by workers most likely to be displaced. Capacity building measures by the State can help bridge this gap and ensure displaced workers are equipped with the necessary skills to find alternative employment in an

evolving economy.

Additionally, the State must also mandate that businesses have periodic human oversight over AI software that workers interact with directly. Principle 3 (c) of the UNGPs notes the State's duty in providing guidance to businesses on how to respect human rights throughout their operations. Directives to businesses explaining the need for human oversight will be a step in this direction. It will help reduce the possibility of bias and discrimination and ensure effective implementation of AI software from a human rights standpoint.

Pillar 2:

Businesses must look to reskill their workforces

While automation will bring about efficiency gains for businesses, it will also increase the demand for technological, social and emotional skills in different activities. While reskilling can be time and resource intensive, studies show that it can offer a higher return on investment in the long term than hiring from outside (McKinsey 2019). The study by McKinsey shows that reskilling can have tangible benefits through increasing goodwill in customers and employees which translates into a drop in business transformation failure. Reskilling existing employees also allows businesses to retain institutional knowledge and saves time taken to onboard new employees and the time they need to acquaint themselves with the culture and ethic of the business. By identifying the new type of skills that will be required and equipping the existing workforce with them, businesses can ensure compliance with Principle 13 (a) of the UNGPs which notes the responsibility of businesses to avoid causing or contributing to adverse human rights impacts through their own activities.

Principle 17 of the UNGPs specifically highlights that in order to identify, prevent and mitigate adverse human rights impacts, business enterprises should carry out HRDD. With regard to deployment of AI software for workforce management, businesses must put in place measures for regular oversight over tasks and decisions carried out by the software. This will also help businesses receive feedback from workers about their experience in using the software and the possible invisible impacts of the software on workers. Doing so will help businesses

respect Principle 20 of the UNGPs by verifying whether adverse human rights impacts are being addressed. Businesses can then work in tandem with software providers to acquaint their workers with the working of the software, and improve the software based on worker feedback.

Risk 1: Loss of Jobs

Protect

State
- Implement skilling policies that focus on improving competencies of workers.

Unions and Civil Society
- Conduct upskilling workshops for workers.

Respect

Business
- Undertake upskilling initiatives for employees to equip them with skills for new jobs.

Remedy

State
- Provide effective and meaningful access to judicial remedies for displaced workers
- Provide social security protection for displaced workers
- Provide severance and care packages for displaced workers.

Business
- Setting up of internal grievance redressal mechanisms to resolve disputes raised vis-à-vis loss of jobs by workers.

Unions and Civil Society
- Build awareness and capacity of workers to access State and non-State remedies effectively.

Risk 2: Erosion of worker autonomy and risk of discrimination

Protect

State

- Mandate human intervention in the use of AI workforce management systems.

Respect

Business

- Ensure periodic intervention/oversight by management regarding AI workforce management systems
- Engage with workers to understand the issues they face with these systems.

Remedy

State

- Establish mediation and conciliation mechanisms that can be accessed by workers displaced due to AI deployment.

Business

- Establish grievance redressal mechanisms that involve managerial personnel
- Allow for correction of erroneously captured information as soon as possible.

Unions and Civil Society

- Engage with workers and AI system designers to help inform design of better workforce management systems.

Gig Work

Risk mitigation strategies, according to the UNGPs' 'Protect, Respect and Remedy' framework, can broadly be summarised as:

- The State should focus on instituting a robust legal regime that ensures adequate protection of rights of workers.
- Business should allow workers to have transparency over the functioning of the algorithm in addition to providing social security benefits.
- Remedy frameworks should be worker-centric, focussing on building awareness and access to remediation frameworks (State and non-State) amongst workers regarding their data and rights, access to social security benefits and facilitating grievance redressal.

Pillar 1:

The State must put in place a robust legal regime to protect workers' rights

While the 2020 Labour Codes are a good start in recognising gig workers' rights to social security protections, the State must strive to operationalise this framework to ensure that the workers actually receive the benefits. This is in line with Principle 3 (a) of the UNGPs which notes that States should not only enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights but also periodically assess the adequacy of such laws and address any gaps. Given this, the onus is also on the State to go beyond this to mandate that on-demand companies provide additional safety measures to women and also put in place effective grievance redressal mechanisms. In addition to this, the State can mandate that the contracts between gig workers and companies account for the extent of control exerted by companies –

by recognising emoluments such as minimum wages and paid leave. Finally, instituting data protection legislation will provide workers with more rights over their data, helping to reduce the power imbalance between platforms and workers.

Pillar 2:

Business should strive to recognise basic protections for workers and provide transparency to them, and recognise this in contracts

Expert interview analysis highlighted that on-demand platform companies are able to use algorithmic opaqueness to further aggravate the power divide between the company and workers. This allows the company to use data generated by the workers to optimise their algorithms to the detriment of the very workers. Indeed, the nature of the relationship between the company and workers is more akin to a traditional employer-employee relationship than that of an independent contractor. This is also being recognised by courts in various other jurisdictions with regard to certain platforms.

To begin with, companies must ensure that workers are entitled to basic social security protections and a minimum wage, in line with Principle 12 of the UNGPs which alludes to the International Labour Organization's Declaration on Fundamental Principles and Rights at Work. Companies must also provide transparency to workers regarding how their ratings are calculated and how work is allocated by the algorithm. Transparency will help improve the working conditions of workers and can also have knock-on effects on worker safety as well as grievance redressal. In addition to this, the UNGPs, in Principle 22, note the necessity for businesses to have legitimate processes in place for grievance redressal. Instituting a grievance redressal mechanism that is worker-friendly, effective and transparent and takes into account social inequities will go a long way in addressing the human rights concerns faced by workers in this domain.

Risk 1: Inadequacy of income and poor working conditions

Protect

State

- Implement robust regulations on minimum wages and paid leave for gig workers
- Mandate additional safety measures for women.

Unions and Civil Society

- Industry bodies (such as NASSCOM and ASSOCHAM) should issue codes of conduct or best practices to be observed by companies to ensure fair working conditions and wages for gig workers.

Respect

Business

- Revise contracts with workers to recognise the nature of control exercised by the business
- Ensure minimum wages based on global standards
- Ensure provision of paid leave to workers
- Provide transparency to workers in the determination of their ratings
- Institute mechanisms for wage cover for wages lost owing to grievance redressal.

Remedy

State

- Provide access to judicial and quasi-judicial resolution mechanisms which account for the nature of gig work and go beyond evaluating it purely on contractual terms.

Business

- Establish transparent, accessible and effective remediation channels
- Engage with unions regarding demands for better working conditions.

Unions and Civil Society

- Advocate workers' right to transparency in ratings.

Risk 2: Worker surveillance

Protect	**State** • Institute data protection legislation that recognises workers' rights over their data.
Respect	**Business** • Adhere to strict standards of data protection in collection, processing and sharing. • Have periodic training of workers in free, prior and informed consent on data collection.
Remedy	**Business** • Provide workers with access to the data collected by the business about the worker as well as the uses such data is being put to • Allow workers opportunity to correct erroneous data. **Unions and Civil Society** • Conduct events to improve data literacy amongst workers.

Risk 3: Absence of social security

Protect

State

- Operationalise the social security framework in the 2020 Labour Codes.
- Mandate that businesses must revise contracts to provide social security protection.

Respect

Business

- Provide legally mandated social security protections to workers on a par with protections to employees.
- Revise worker contracts to include provisions for social security.

Remedy

State

- Provide workers with equitable and meaningful access to judicial remedies for disputes regarding social security benefits.

Business

- Institute a separate transparent internal grievance redressal mechanism to address grievances and disputes related to social security benefits.

Unions and Civil Society

- Encourage worker awareness on social security protection as well as abuse of their data.

Risk 4: Risk to effective remedy and grievance redressal

Protect	**State** • Mandate institution of effective human-led grievance redressal mechanisms by businesses.
Respect	**Business** • Institute mechanisms for explanation of decision-making by the algorithm to workers.
Remedy	**State** • Conduct periodic reviews of proceedings of businesses' grievance redressal mechanisms to ensure effective and transparent functioning. **Business** • Provide workers with a functional grievance redressal system that does not rely on AI and gives workers an adequate opportunity to be heard.

06 /

References

AIRS Working Group. (n.d.). Artificial Intelligence Risk & Governance. Artificial Intelligence for Business. Retrieved December 13, 2021, from https://ai.wharton.upenn.edu/artificial-intelligence-risk-governance/

Allison-Hope and Hodge (2018). Artificial Intelligence: A Rights-Based Blueprint for Business Paper 2: Beyond the Technology Industry. BSR.or. https://www.bsr.org/reports/BSR-Artificial-Intelligence-A-Rights-Based-Blueprint-for-Business-Paper-02.pdf

Arpey NC, Gaglioti AH, Rosenbaum MEJ Prim Care Community Health. 2017 Jul; 8(3):169-175.

Bailey, Rishab, Smriti Parsheera, Faiza Rahman, and Renuka Sane. (2018). Disclosures in Privacy Policies: Does 'Notice and Consent' Work? NIPFP Working Paper No. 246. National Institute of Public Finance and Policy. https:// www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

Athreya, B. (2020). Slaves to Technology: Worker control in the surveillance economy. Anti-Trafficking Review. https://www.antitraffickingreview.org/index.php/atrjournal/article/view/490/383

Bala, S. (2021, May 13). Already under massive stress from the virus, more Indian workers turn to 'gig economy' livelihoods. CNBC. https://www.cnbc.com/2021/05/14/india-jobs-workers-turn-to-gig-economy-jobs-amid-coronavirus-crisis.html

Balaji, Sindhuja. (2020). AI filling the gap in India's abysmal physician:patient ratio. IndiaAI. gov.https://indiaai.gov.in/article/ai-filling-the-gap-in-india-s-abysmal-physician-patient-ratio

Basu, A. (2020, April 20). E-shopping to mobile recharges, Indian banks have a wealth of data to check creditworthiness. Quartz. https://qz.com/india/1841163/ai-big-data-can-help-indian-banks-move-beyond-just-credit-score/

BEUC Position Paper. (2018). Automated Decision Making and Artificial Intelligence- A Consumer Perspective. https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf

Bitterman, D., Aerts, H., & Mak, R. (2020). Approaching autonomy in medical artificial intelligence. https://www.thelancet.com/action/showPdf?pii=S2589-7500%2820%2930187-4

Chami, N., & Sanjay, S. (2020, December 23). A data rights agenda for platform and gig economy workers. Hindustan Times. https://www.hindustantimes.com/analysis/a-data-rights-agenda-for-platform-and-gig-economy-workers/story-9ZtpX9kavVSN5TNQcE289M.html

Chandran, R. (2021, June 9). As AI-Based Loan Apps Boom in India, Some Borrowers Miss Out. The Wire. https://thewire.in/tech/as-ai-based-loan-apps-boom-in-india-some-borrowers-miss-out

Childress, J. F. & Beauchamp, T. L. Principles of biomedical ethics. (Oxford University Press, 2001).

Chitkara, R., & Tandon, D. (2021). India's Gig Economy: How the 'No Rules' Industry Renders Workers Helpless. The Quint. https://www.thequint.com/voices/opinion/indias-gig-workers-a-study-shows-how-companies-evade-law-responsibility

Christopher, N. (2021, January 27). Payday lenders are using illegal apps on Google Play to harass and publicly shame borrowers in India. Rest of World. https://restofworld.org/2021/debt-and-shame-via-google-play/

CSBC AND Busara Research. (2020). Behavioural Experiments in Data Privacy. https://busaracenter.org/report-pdf/InAct_Report.pdf

Danah boyd, Karen Levy, and Alice Marwick, "The Networked Nature of Algorithmic Discrimination," in Data and Discrimination: Collected Essays, ed. Seeta Peña Gangadharan (New America, 2014), 53–57.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. Reuter.com. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Deloitte Insights. (2019, July 19). Using predictive analytics in health care. https://www2.deloitte.com/us/en/insights/topics/analytics/predictive-analytics-health-care-value-risks.html

Deutsch, A., & Sterling, T. (2021, September 13). Uber drivers are employees, not contractors, says Dutch court. Reuters. https://www.reuters.com/world/europe/dutch-court-rules-uber-drivers-are-employees-not-contractors-newspaper-2021-09-13/

Dilmegani, C. (2020, October 2). 90+ Chatbot / Conversational AI Statistics: Market Size, Adoption. https://research.aimultiple.com/chatbot-stats/

Dunga, C. (2020). How effective is artificial intelligence in removing racial bias in hiring?. Quartz.com. https://qz.com/work/1923587/can-artificial-intelligence-solve-racism/

Dvara Research. (2021). A Convening on 'Emerging Customer Risks in Digital Lending in India. https://www.dvara.com/research/wp-content/uploads/2021/08/A-Convening-on-Emerging-Customer-Risks-in-Digital-Lending-in-India.pdf

ElectricDirect. (2021, May 17). Are Robots Taking Over Our Jobs? https://www.electricaldirect.co.uk/blog/robots-taking-over-jobs

European Commission. 2021. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

Fairworks. (2020). Fairwork India Ratings 2020: Labour Standards in the Platform Economy. Fairworks. https://fair.work/wp-content/uploads/sites/131/2020/12/Fairwork_India_2020_report.pdf

Fletcher, R. R., Nakeshimana, A., & Olubeko, O. (2021). Addressing Fairness, Bias, and Appropriate Use of Artificial Intelligence and Machine Learning in Global Health. Frontiers in Artificial Intelligence, 3, 116. https://doi.org/10.3389/frai.2020.56180

Gartner. (2020, February 27). Top CX Trends for CIOs to Watch. https://www.gartner.com/smarterwithgartner/top-cx-trends-for-cios-to-watch

Gianfrancesco, M. A., Tamang, S., Yazdany, J., & Schmajuk, G. (2018). Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data. JAMA Internal Medicine, 178(11), 1544–1547. https://doi.org/10.1001/jamainternmed.2018.3763

Giordano, C., Brennan, M., Mohamed, B., Rashidi, P., Modave, F., & Tighe, P. (2021). Accessing Artificial Intelligence for Clinical Decision-Making. Frontiers in Digital Health. 3, 65. https://doi.org/10.3389/fdgth.2021.645232

Global Market Insights. (2021). Artificial Intelligence (AI) in Retail Market (p. 280).

Gupta, D. A. (2018, January 2). Transforming The Face Of Healthcare One Step At A Time, Predictive Analytics Is The Hottest Trend Now. Analytics India Magazine. https://analyticsindiamag.com/transforming-face-healthcare-one-step-time-predictive-analytics-hottest-trend-now/

Gupta, S., & Natarajan, S. (2019). Gender and Future of Workers. Medium.com. https://medium.com/aapti/gender-and-future-of-workers-136e351266c0

Haritas, Bhragu (2019). Healthcare analytics can minimise misdiagnosis, malpractice, unexpected costs: CTO, THB. Economic Times. https://cio.economictimes.indiatimes.com/news/strategy-and-management/healthcare-analytics-can-minimise-misdiagnosis-malpractice-unexpected-costs-cto-thb/71250763

IBEF. (2021, May 5). Emergence of India's Gig Economy. https://www.ibef.org/blogs/emergence-of-india-s-gig-economy

IBM. (n.d.). The coming AI revolution in retail and consumer products. Retrieved December 13, 2021, from https://www.ibm.com/downloads/cas/NDE0G4LA

IBM. (n.d.) What is automation? Retrieved December 13, 2021, from https://www.ibm.com/topics/automation

ICO. (n.d.) What is automated individual decision-making and profiling?ICO.uk.org. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id2

IFMR Finance Foundation. (2017, July 3). Insights from the "Digital Credit Roundtable." Dvara Research Blog. https://www.dvara.com/research/blog/2017/07/03/insights-from-the-digital-credit-roundtable-hosted-by-the-future-of-finance-initiative/

India Literacy Project. (2021, August 4). Career Guidance for students on WhatsApp. https://www.ilpnet.org/csmchatbot/

Indian Express (2016). Maharashtra website hacked: Diagnostic lab details of 35,000 patients leaked. https://indianexpress.com/article/india/diagnostic-lab-details-of-35000-patients-leaked-hiv-reports-4407762/

Intel. (n.d.). How Predictive Analytics Impacts the Future of Healthcare. Intel. Retrieved December 13, 2021, from https://www.intel.com/content/www/in/en/healthcare-it/predictive-analytics.html

Internet Freedom Foundation. (2021, November 8). Digital lending and small borrowers! #PrivacyOfThePeople. Internet Freedom Foundation. https://internetfreedom.in/privacyofthepeople-small-borrowers-and-digital-lending-apps/

Jha, D (2021, August 25). Integration of AI in Financial Services. Outlook India. https://www.outlookindia.com/outlookmoney/fintech/integration-of-ai-in-financial-services-8476

Johnston, S. C. Anticipating and Training the Physician of the Future: The Importance of Caring in an Age of Artificial Intelligence. Acad. Med 93, 1105–1106 (2018).

Kasliwal, R. (2020), Gender and the Gig Economy: A qualitative study of Gig platforms for women workers. ORF Issue Brief.https://www.orfonline.org/research/gender-and-the-gig-economy-a-qualitative-study-of-gig-platforms-for-women-workers-65948/

Kassner, MP., (2021). We need to pay attention to AI bias before it's too late. Tech Republic. com.https://www.techrepublic.com/article/we-need-to-pay-attention-to-ai-bias-before-its-too-late/

Klein, A. (2019, April 11). Credit denial in the age of AI. Brookings. https://www.brookings.edu/research/credit-denial-in-the-age-of-ai/

Klein, A. (2020, July 10). Reducing bias in AI-based financial services. Brookings. https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/

KPMG. (2020). Living in an AI World 2020 Report: Retail Insiders. https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/retail-living-in-an-ai-world.pdf

Kulkarni, A., Narayan, S. and Punia, S. (2019). User Perspectives on Privacy and Data Protection. [online] Cuts-ccier.org. https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

Lipsmeier, F. et al. Evaluation of smartphone-based testing to generate exploratory outcome measures in a phase 1 Parkinson's disease clinical trial: remote PD testing with smartphones. Mov. Disord. 33, 1287–1297 (2018).

Lynn, L. A. (2019). Artificial intelligence systems for complex decision-making in acute care medicine: A review. Patient Safety in Surgery, 13(1), 6. https://doi.org/10.1186/s13037-019-0188-2

Manrai AK, Funke BH, Rehm HL, Olesen MS, Maron BA, Szolovits P, Margulies DM, Loscalzo J, Kohane. Genetic Misdiagnoses and the Potential for Health Disparities. ISN Engl J Med. 2016 Aug 18; 375(7):655-65.

Matthan, R. (2017), Beyond Consent: A New Paradigm for Data Protection. Takshahila Institution. https://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf

McCradden, M. D., Joshi, S., Mazwi, M., & Anderson, J. A. (2020). Ethical limitations of algorithmic fairness solutions in health care machine learning. The Lancet Digital Health, 2(5), e221–e223. https://doi.org/10.1016/S2589-7500(20)30065-0

McKinsey. (2020, November 17). Global survey: The state of AI in 2020. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020

Meyers, Z. (2021, August 10). Driving uncertainty: Labour rights in the gig economy. https://www.cer.eu/sites/default/files/insight_ZM_gig_10.8.21.pdf

Miller, K. (2021, July 6). Future of Work: Beyond Bossware and Job-Killing Robots. Stanford HAI. https://hai.stanford.edu/news/future-work-beyond-bossware-and-job-killing-robots

Morley, J., Machado, C. C. V., Burr, C., Cowls, J., Joshi, I., Taddeo, M., & Floridi, L. (2020). The ethics of AI in health care: A mapping review. Social Science & Medicine, 260, 113172. https://doi.org/10.1016/j.socscimed.2020.113172

Murray, S., Wachter, R., & Cucina, R,. (2020). Discrimination By Artificial Intelligence In A Commercial Electronic Health Record—A Case Study. Health Affairs.com. https://www.healthaffairs.org/do/10.1377/forefront.20200128.626576/full/

NASSCOM. (2020). Indian retail: AI imperative to data-led disruptive growth.

NASSCOM. (2021). How AI Is Transforming The Future Of Healthcare In India.

Natarajan, S., Mishra, K., Taylor, Dr. A., & Mohamed, S. (n.d.). AI_Data_Labelling_Report_DIGITAL_25FEB1033.pdf. Retrieved December 13, 2021, from https://uploads.strikinglycdn.com/files/7d492f74-a51f-423b-bf5d-65c9f88eee06/AI_Data_Labelling_Report_DIGITAL_25FEB1033.pdf

Natarajan, S & Sharma, L. (2021). Opinion: Investing for inclusive tech. Economic Times. https://government.economictimes.indiatimes.com/news/digital-india/opinion-investing-for-inclusive-tech/82013516

Natrajan, S., & Nasiripour, S. (2019, November 10). Viral Tweet About Apple Card Leads to Goldman Sachs Probe. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-11-09/viral-tweet-about-apple-card-leads-to-probe-into-goldman-sachs

Newlands, G. (2020). Algorithmic Surveillance in the Gig Economy: The Organization of Work through Lefebvrian Conceived Space. Sage Pub Journals. https://journals.sagepub.com/doi/full/10.1177/0170840620937900

O'Kane, S. (2021, March 16). Uber drivers in the UK will now get minimum wage and paid vacation after a big court win. The Verge. https://www.theverge.com/2021/3/16/22334771/uber-uk-drivers-workers-benefits-employees-decision

Parry, C. M., & Aneja. (2020, July 30). Artificial Intelligence for Healthcare: Insights from India. Chatham House – International Affairs Think Tank. https://www.chathamhouse.org/2020/07/artificial-intelligence-healthcare-insights-india-0/2-ai-and-healthcare

Paul, Y., Hickok, E., Sinha,A., & Tiwari, U. (2018). Artificial Intelligence in the Healthcare Industry in India. Centre for Internet & Society. https://cis-india.org/internet-governance/ai-and-healthcare-report

Philips India. (2021). A resilient future: Healthcare leaders look beyond the crisis. https://images.philips.com/is/content/PhilipsConsumer/Campaigns/CO20210803_Fhi_India/philips_future_health_index_2021_report_healthcare_leaders_look_beyond_the_crisis_india.pdf?_gl=1*18vyw5l*_ga*NTY4MjcwNDg3LjE2MzI0ODE0OTg.*_ga_2NMXNNS6LE*MTYzMjQ4MTQ5Ny4xLjEuMTYzMjQ4MTUxMC40Nw..&_ga=2.181494759.1343721542.1632481498-568270487.1632481498

Prabhakar, Tarunima., Weber, Steve. (2020(a)). Financial Inclusion as A Fairness Criterion in Credit Risk Assessment https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3579695

Prabhakar, Tarunima., Weber, Steve. (2020 (b)). Alternative Lending in A Digital Age: A Comparative Case Study in Regulation Across India and The United States.

Prasad, P. (2018). Driven by targets, delivery boys violate rules. The New Indian Express. https://www.newindianexpress.com/cities/bengaluru/2018/dec/13/driven-by-targets-delivery-boys-violate-rules-1910774.html

Prasad, S. (2021). Addressing Bias Is Key for the Adoption of AI in Healthcare. CXOToday.com. https://www.cxotoday.com/ai/addressing-bias-is-key-for-the-adoption-of-ai-in-healthcare/

PUDR. (2021). Behind the Veil of Algorithms: Invisible Workers: A Report on Workers in the 'Gig' Economy. https://pudr.org/sites/default/files/2021-12/PUDR%20report%20on%20gig%20workers-%20Behind%20the%20Veil%20of%20Algorithms.pdf

PWC. (2021). Understanding algorithmic bias and how to build trust in AI. PWC.com. https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html

PWC. (n.d.). Sizing the prize: What's the real value of AI for your business and how can you capitalise? PWC.Com. Retrieved December 13, 2021, from https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Raibagi, K. (2021). The Plight Gig Workers In An Algorithm-Driven World, Analytics India Mag. https://analyticsindiamag.com/the-plight-of-gig-workers-in-an-algorithm-driven-world/

Rawat, A. (2019). Swiggy, Zomato Delivery Boys Breaking Traffic Rules; Police Blame Unfair Incentives. Inc42.com. https://inc42.com/buzz/swiggy-zomato-delivery-boys-breaking-traffic-rules-police-blame-unfair-incentives/

Rao, M. M. (2019, August 30). The 'gig' economy is creating lakhs of jobs, but workers don't see a future. The Hindu. https://www.thehindu.com/business/Economy/the-gig-economy-is-creating-lakhs-of-jobs-but-workers-dont-see-a-future/article29299673.ece

Rao, P. (n.d.). Radiology Management, ICU Management, Healthcare IT, Cardiology Management, Executive Management. HealthManagement. Retrieved December 13, 2021, from https://healthmanagement.org/c/healthmanagement/issuearticle/ai-and-healthcare-technology-in-india-opportunities-challenges-and-emerging-trends

Raso, F., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018, September). Artificial Intelligence & Human Rights: Opportunities & Risks. https://cyber.harvard.edu/sites/default/files/2018-09/2018-09_AIHumanRightsSmall.pdf

Rathi, A., & Tandon, A. (n.d.). Platforms-power-and-politics-pdf.pdf. Retrieved December 13, 2021, from https://cis-india.org/raw/platforms-power-and-politics-pdf

Ray, K. (2018, September 21). 4,300 Indians die daily due to poor hospital care.Deccan Herald. https://www.deccanherald.com/opinion/panorama/4300-indians-die-daily-due-692128.html

Research and Markets (2019). Artificial Intelligence (AI) in Healthcare Market in India (2018-2023).

Rice, L and Swensik, D (2013). Discriminatory Effects of Credit Scoring on Communities of Color. 46 Suffolk University Law Review 935.

Richardson, J., Smith, C., Curtis, S., Watson, S., Zhu, X., Barry, B., & Sharp, R. (2021, September 21). Patient apprehensions about the use of artificial intelligence in healthcare | npj Digital Medicine. https://www.nature.com/articles/s41746-021-00509-1#ref-CR19

Rizzi, A and Kumari, T (2021). Trust of Data Usage, Sources, and Decisioning: Perspectives From Rwandan Mobile Money Users. Centre for Financial Inclusion. https://www.centerforfinancialinclusion.org/_preview/43393/71f6130849

Roy, S. (2021, February 28). Artificial Intelligence: Global scenario versus Indian landscape. Cnbctv18.Com. https://www.cnbctv18.com/views/artificial-intelligence-global-scenario-versus-indian-landscape-8452151.htm

Sarkar, K. (2020, October 12). Under new labour code, an Uber driver can be both gig and platform worker. It's a problem. ThePrint. https://theprint.in/opinion/under-new-labour-code-an-uber-driver-can-be-both-gig-and-platform-worker-its-a-problem/521628/

Siddiqui, Z., & Zhou, Y. (2021). How the platform economy sets women up to fail. Rest of World.com https://restofworld.org/2021/global-gig-workers-how-platforms-set-women-up-to-fail/

Singh, A., & Prasad, S. (2020, April 13). Artificial Intelligence in Digital Credit in India. Dvara Research Blog. https://www.dvara.com/research/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/

Sonne, Lina. (2020). What do we Know about Women's Mobile Phone Access and Use? A review of evidence. Dvara Research Working Paper Series No. WP-2020-03, https://www.dvara.com/research/ wp-content/uploads/2020/06/What-Do-We-KnowAbout-Womens-Mobile-Phone-Access-Use-A-reviewof-evidence.pdf.

Sun, S. (2021). Share of mobile phone owners in India in 2019, by gender and type. Statista. https://www.statista.com/aboutus/our-research-commitment/2834/shangliao-sun

Thomas, S. (2020, September 8). Report: State of Artificial Intelligence in India - 2020. Analytics India Magazine. https://analyticsindiamag.com/report-state-of-artificial-intelligence-in-india-2020/

United Nations. Human Rights. https://www.un.org/en/global-issues/human-rights.

Verghese, A., Shah, N. H. & Harrington, R. A. What This Computer Needs Is a Physician: Humanism and Artificial Intelligence. JAMA 319, 19–20 (2018).

Vidal. (2020, September 29). Data Privacy Concerns Influence Financial Behaviors in India, Kenya. https://www.cgap.org/blog/data-privacy-concerns-influence-financial-behaviors-india-kenya

Weber GM, Adams WG, Bernstam EV, Bickel JP, Fox KP, Marsolo K, et al. Biases introduced by filtering electronic health records for patients with "complete data." J Am Med Inform Assoc. (2017) 24:1134–41. doi: 10.1093/jamia/ocx071

WHO Guidance. (2021, June 28). Ethics and governance of artificial intelligence for health. https://www.who.int/publications-detail-redirect/9789240029200

World Economic Forum. (2020). The Future of Jobs Report 2020. https://www.weforum.org/reports/the-future-of-jobs-report-2020

Annexure A – Policy Brief

This policy brief has been developed as part of the United Nations Development Programme's Business and Human Rights Asia programme (B+HR Asia), which aims to strengthen human rights conditions in business operations and supply chains to facilitate sustainable economic growth and increased levels of trade and investment.

This brief outlines the findings of a larger report on the human rights risks posed by the growth of artificial intelligence (AI) in the healthcare, financial services, traditional retail and gig work sectors. The brief argues that AI holds great potential for the realisation of India's social and economic goals. However, a broad set of actions needs to be undertaken by the Government of India (GOI) to mitigate human rights risks posed by the private sector's increased and largely unregulated deployment of AI.

The brief recognises the complementary but differentiated responsibilities of the government and business in the area of human rights. As such, the recommendations provided below are informed by the 'Protect, Respect and Remedy' framework of the United Nations Guiding Principles on Business and Human Rights (UNGPs) with a particular focus on the State's duty to protect human rights (Pillar 1).

Introduction: Need for a human rights-sensitive approach to AI deployment

The COVID-19 pandemic accelerated the adoption of artificial intelligence (AI) technologies across several domains in India. Businesses that had invested in AI technology pre-COVID were better equipped to tackle the challenges posed by the pandemic and to transition into a digitised world

with ease[1]. By many measures, AI will play a significant role in powering economic growth in India over the long term[2].

Growing digitisation and increased capital flows are fuelling AI's uptake across sectors that are witnessing efficiency gains from its use. It also provides a facilitative environment for steady and sustainable economic growth through long-term investments. Research indicates that a substantial increase in deployment of AI by Indian firms has led to a 2.5% increase in GDP[3]. It has been highlighted that the investment of INR 7,000 crore in the AI programme approved by the Ministry of Finance in 2020 can translate into spillover benefits of USD 85.77 billion for the Indian economy[4].

Responsible and ethical deployment of AI by businesses, especially in critical sectors such as healthcare and finance, contribute to the fulfilment of State objectives of financial and healthcare inclusion by increasing access to formal credit and quality healthcare, respectively. The gig economy, which predominantly relies on use of AI algorithms for mediation of work, has had an enormous impact in India and the pandemic has only accelerated it. India's gig sector is expected to increase to USD 455 billion at a CAGR of 17% by 2024 and has the potential to expand to at least twice the pre-pandemic estimates[5]. There are also expected to be 350 million gig jobs in India by 2025[6].

Given the significant impact of AI uptake on GDP and economic growth, the State has a clear interest in driving AI adoption across sectors. It has to play a more active role by facilitating innovation and providing a thriving business environment for AI deployment.

However, AI deployment involves significant human rights risks, particularly in the financial services, healthcare, retail, and gig work

[1] PwC (2020), AI: An opportunity amidst a crisis. Available at: https://www.pwc.in/assets/pdfs/data-and-analytics/ai-an-opportunity-amidst-a-crisis.pdf
[2] Ibid. NITI Aayog (2021), Responsible AI – Approach Document For India: Part 2 – Operationalizing Principles For Responsible AI. Available at: https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf
[3] Kathuria, R., Kedia, M., Kapilavai, S. (2021). Implications of AI on the Indian Economy. ICRIER Report. Available at: http://icrier.org/pdf/ES/ES-Implications_of_AI_on_the_Indian_Economy.pdf
[4] Ibid.
[5] IBEF Knowledge Centre (2021). Emergence of India's Gig Economy. IBEF. Available at: https://www.ibef.org/blogs/emergence-of-india-s-gig-economy
[6] Bala, S. (2021). Already under massive stress from the virus, more Indian workers turn to 'gig economy' livelihoods. CNBC. Available at: https://www.cnbc.com/2021/05/14/india-jobs-workers-turn-to-gig-economy-jobs-amid-coronavirus-crisis.html

sectors. Human rights risks are further exacerbated for marginalised populations — including women — given their vulnerability and the inherent power imbalances in group dynamics that predispose them to face risks of bias and discrimination.

The intersection of AI with human rights is admittedly a complex topic to understand and analyse, and requires the State to carefully calibrate policy to both protect human rights and maximise AI's potential to create jobs and alleviate poverty. Since India seeks to position itself as a dynamic global economy attracting trade and investment, imagining AI deployment that is embedded in human rights framing enables the protection of citizens. It should work in tandem with ongoing initiatives of the State such as 'Responsible AI' and 'Digital India'. Addressing human rights concerns is of utmost importance as we look at AI as a tool that helps us compete with advanced economies by accelerating technological advancement and economic growth.

A multi-phased approach — through both desk research and interviews of experts — to identify harms and build solutions around the use of AI by businesses within the UNGPs' three-pillar framework ('Protect, Respect and Remedy') on business and human rights, was adopted and a three-part study carried out. This dynamic approach ensures that research insights are abreast of real-time changes in the dialogue at the national level.

This brief documents the *unique effects of four types of AI on citizens as consumers and workers* with a focus on financial services, healthcare, retail and gig work, and offers recommendations for the State to mitigate human rights risks caused due to AI deployment in businesses.

	Type of AI	Effect	Sector
Consumers	Profiling and Automated Decision Making	Erosion of market access	Financial services
	Predictive Analysis	Erosion of consumer agency	Healthcare
Labourforce	AI automation	Loss of job	Retail
	AI intermediated work	Worker surveillance	Gig work

Figure 1: Sector selection

The identification of human rights risks was based on an understanding and review of international covenants such as the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights. National legal documents such as the Indian Constitution and various pieces of statutory legislation including the Social Security Code, 2020, and the Personal Data Protection Bill, 2019, were also taken into consideration.

The specific human rights that are threatened across sectors, due to AI deployment, are varied.

Financial services

It can erode the right to privacy, financial access, life, and dignity, further affecting the right to grievance redressal of consumers.

Healthcare

It may enable bias, thus eroding consumers' right to life, individual freedom of choice and autonomy, data privacy, and equality.

Retail

It leads to loss of jobs and risks erosion of worker autonomy which affects their rights to work, a standard of living, and enjoyment of just and favourable conditions of work.

Gig work

It affects the gig workers' rights to privacy, social security, and effective remedy.

The risk mitigation strategies proposed are informed with the three-pillar — 'Protect, Respect and Remedy' — framework of the UNGPs. Adopted in 2011 by the UN Human Rights Council, the UNGPs are the world's most authoritative, normative framework guiding responsible business globally today. This framework provides that States and businesses have shared but also varying responsibilities to ensure that human rights are protected and respected in business operations.

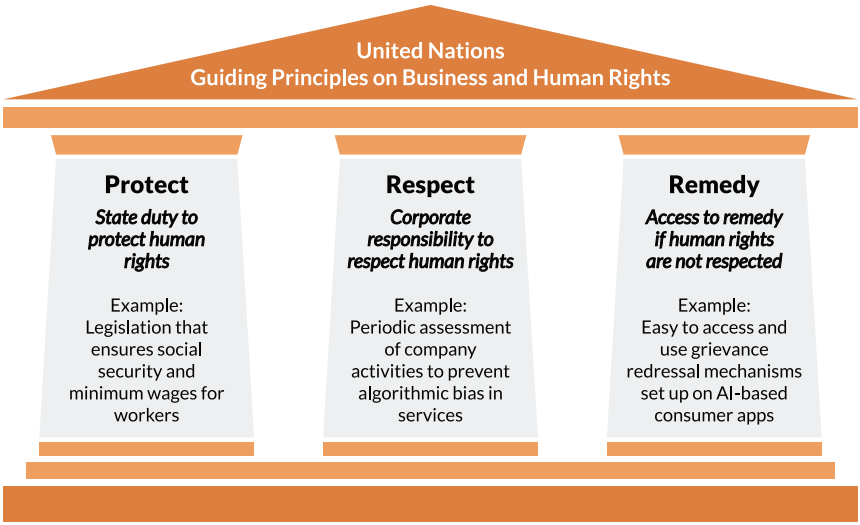


Figure 2: UNGPs' three-pillar framework on business and human rights

Our findings suggest that AI risks and effects cannot be isolated from company policies and regulatory frameworks. AI technology mirrors

company policies and choices, and company preferences are embedded in technology during its development. Regulatory frameworks are foundational to guiding company policy, and their lack fosters environments that disregard human rights. For instance, absence of regulation on digital lending resulted in the flourishing of predatory lending apps which have been the cause of multiple suicides[7]. The recent Reserve Bank of India (RBI) report by the Working Group on digital lending, which stipulates separate legislation preventing illegal lending, reiterates our finding that regulatory overwatch is a must to address human rights concerns[8].

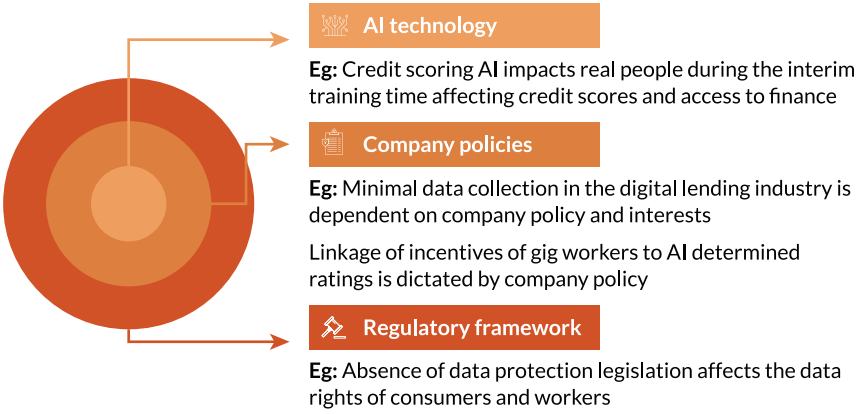


Figure 3: Intersection of AI, company policy and regulatory framework, along with examples across sectors

In conclusion, actions of the State must be cushioned within a framework, such as 'Responsible AI', that respects human rights. Further, its efforts to drive uptake of AI should be complemented by measures that also mitigate the human rights risks that arise due to AI deployment. State intervention in the form of regulation is critical, considering that regulatory frameworks guide business practices surrounding AI deployment.

[7] Mathi, S. (2021). Summary: RBI Report on regulating digital lending and curbing the menace of predatory lending apps. Medianama. Available at: https://www.medianama.com/2021/11/223-summary-rbi-working-group-report-digital-lending/

[8] RBI (2021). Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps. Available at: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189

Unpacking human rights risks

Key Terms

AI automation
The most complex level of automation is artificial intelligence automation. The addition of AI means that machines can "learn" and make decisions based on past situations they have encountered and analysed.

AI based credit scoring
Usage of artificial intelligence to assess the credit risk of a potential borrower by analysing vast amounts of data from many sources.

Predictive Analytics
Predictive analytics is a branch of advanced analytics which in the realm of healthcare transforms patient care, both at individual level and cohort scale, by evaluating historical and real-time data.

Source: IBM, Raso et al. (2018), Deloitte Insights (2019)

AI based credit scoring in *financial services* may lead to human rights risks including

- **Invasion of consumer privacy**

Privacy concerns in India stem from a lack of informed consent and rampant data collection practices in AI-based credit scoring models. First, AI technology is capable of drawing inferences other than determining creditworthiness, that consumers never consented to be drawn by the technology. Experts stated that consumers do not give their informed consent for inferences to be drawn about their sexuality, and religious and political affiliation.

Second, the security risk for Indian consumers is aggravated when we compare the effect of any potential data breach across different financial

institutions. For instance, data breach in a bank will compromise one's financial information whereas data breach of a digital lender's repository will compromise sensitive information about the user such as social media usage, location and contacts history, online behaviour and purchases, in addition to the financial information[9].

It has been reported that a highly successful fintech company in India embedded middleware in music and religious verses streaming apps to collect personal data to assess creditworthiness[10]. AI developers have cited that this is a common business practice in India[11].

- **Loss of financial well-being and exclusion harms**

For AI to determine the creditworthiness of an individual, data science engineers need to decide what measurements (or metrics) are useful to track and assess the individual's financial strength or acumen. However, there is no agreed or authoritative way of determining what metrics are best.

Experts cited several examples of how over-reliance on some metrics may lead to inaccurate or even discriminatory results in India. For instance, in India metrics purely based on online activity are irrelevant and hence discriminatory towards digitally disconnected populations, leading to loss of opportunity to avail of credit. On the other hand, algorithmic models trained on error-ridden data or incomplete data lead to misclassification of individuals as creditworthy, pushing them into debt traps. In India, lenders target young populations as they are predominantly unbanked. Inability to pay back loans affects the CIBIL scores of these youngsters, undermining their ability to seek finance in future from formal institutions such as banks[12].

[9] Internet Freedom Foundation. (2021, November 8). Digital lending and small borrowers! #PrivacyOfThePeople. Internet Freedom Foundation. https://internetfreedom.in/privacyofthepeople-small-borrowers-and-digital-lending-apps/

[10] Sathe, G. (2019). How Sai Baba Was Made To Spy On Your Phone For Credit Ratings, HuffPost. https://www.huffpost.com/archive/in/entry/fintech-apps-privacy-snooping-credit-vidya_in_5d1cbc34e4b082e55373370a

[11] Ibid.

[12] Chandran, R. (2021, June 9). As AI-Based Loan Apps Boom in India, Some Borrowers Miss Out. The Wire. https://thewire.in/tech/as-ai-based-loan-apps-boom-in-india-some-borrowers-miss-out

- **Risks to life and dignity**

Risk to life looms over Indian consumers, given that inaccuracy in prediction pushes borrowers into over-indebtedness — leading to suicide. The risk to life posed by non-predatory apps directly stems from the financial harms borne by consumers due to misclassification by AI-based credit scoring technology.

In India, there is no regulation of digital lending which allows both illegal (predatory) and legal (non-predatory) apps to exist. Further, in the event that non-predatory apps fail to differentiate themselves from their predatory counterparts, consumers are pushed into the traps of predatory lenders. For instance, a woman attempted suicide when she was faced with demands for nude pictures after defaulting on loan repayment. The app was a predatory app that used the same domain name as a non-predatory one[13].

- **Lack of grievance redressal**

An explanation of a decision is key to seeking effective remedy and grievance redressal. In the absence of explanations for decisions, consumers cannot question or dispute the decisions[14]. In traditional models of credit lending in India, consumers are afforded the right to know the reason for denial of credit, under the Reserve Bank of India norms applicable to banks. However, the same right does not extend to algorithmic decisions made by digital lenders.

Further, experts interviewed for this report noted that businesses in India do not hesitate to make decisions explainable to consumers but, given the complexity of AI, sometimes they become indecipherable for the layperson. However, even if algorithms are explainable, businesses hesitate to explain the workings of their algorithms to regulators given the lack of intellectual property safeguards and proprietary concerns in India.

[13] Christopher, N. (2021, January 27). Payday lenders are using illegal apps on Google Play to harass and publicly shame borrowers in India. Rest of World. https://restofworld.org/2021/debt-and-shame-via-google-play/

[14] McCradden, M. D., Joshi, S., Mazwi, M., & Anderson, J. A. (2020). Ethical limitations of algorithmic fairness solutions in health care machine learning. The Lancet Digital Health, 2(5), e221–e223. https://doi.org/10.1016/S2589-7500(20)30065-0

Human rights risks emerging from the use of predictive analytics AI in *healthcare* (e.g. AI-based prediction of breast cancer) leads to deteriorated patient care. The three key risks are:

- **Likelihood of bias and discrimination affecting patients as underrepresented data about certain populations leads to inaccurate predictions**

Risk of bias and discrimination arise from issues related to data quality. Expert interview analysis indicates three primary reasons as cause for biased and discriminatory datasets – lack of diverse datasets, lack of continuous algorithmic training, and presence of untrustworthy sources. Experts noted that populations in India will be particularly vulnerable to biased and unfair algorithms as it is a low and middle income country characterised by lack of regulation, technical expertise and existing social biases against minority groups. When data about certain populations does not exist in sufficient numbers, it leads to uninformative predictions for minority populations — leaving those predictions applicable to only majority populations.

Misdiagnosis is the primary adverse health outcome of biased datasets. Each country has its own patterns of diseases most commonly prevalent. Similarly, in India, cardiovascular diseases affect people much earlier, in comparison to populations in middle and high income countries[15]. Given that doctors usually diagnose heart attacks based on symptoms experienced by men, any AI developed to diagnose heart attacks will underdiagnose Indian women[16].

- **Loss of patient and doctor autonomy**

Expert interview analysis indicates that inability of the doctor and patient to understand how and why the AI arrived at a particular decision hampers their autonomy, threatening AI adoption.

Research in India by the Centre for Internet and Society indicates that assistive AI technology is most likely to be adopted by the medical fraternity without any resistance as compared to AI technology that

[15] Prasad, S. (2021). Addressing Bias Is Key for the Adoption of AI in Healthcare. CXOToday.com. https://www.cxotoday.com/ai/addressing-bias-is-key-for-the-adoption-of-ai-in-healthcare/
[16] Ibid.

seeks to replace doctors[17]. Experts noted that several issues unfold that ultimately threaten doctor autonomy. For instance, doctors become increasingly concerned that conflicting decisions affect their ability to provide satisfactory care as a result of their diminished confidence in the caregiving pathway.

Patient autonomy, one of the core principles of medical ethics, is also threatened when patients are deprived of the opportunity to choose whether AI should be used in the caregiving pathway or not. Experts stated that information asymmetry about AI deployment and ambiguous medical liability regulation affect patient confidence.

- **Loss of data privacy**

The impact of unfettered health data collection and its invisible frameworks of usage is grave for patients and users of health apps in India. Research in India suggests that AI enables continuous behavioural monitoring and facilitates rampant collection of data through the notice and consent mechanism, aggravating the threat to privacy[18].

The current legal framework lacks enforcement, resulting in non-compliance with data privacy norms. For instance, a diagnostic laboratory did not take any action to secure sensitive patient medical data against hacking, resulting in a data leak of medical records of 35,000 patients[19].

Most simple tasks will be replaced due to AI automation in *retail* leading to

- **Job loss**

Review of extant literature along with conversations with experts indicated that the retail sector, especially in India, has a very high percentage of jobs that are low-skill and are based on basic pattern recognition. This places these jobs in the retail sector at a very high risk of being replaced by

[17] Paul, Y., Hickok, E., Sinha, A., & Tiwari, U. (2018). Artificial Intelligence in the Healthcare Industry in India. The Centre for Internet and Society. https://cis-india.org/internet-governance/ai-and-healthcare-report
[18] Ibid.
[19] The Indian Express (2016). Maharashtra website hacked: Diagnostic lab details of 35,000 patients leaked. https://indianexpress.com/article/india/diagnostic-lab-details-of-35000-patients-leaked-hiv-reports-4407762/

AI-led automation.

The resulting combination of automated systems and a lack of reskilling measures crystallises the loss of jobs for human workers in the retail sector.

- **Threats to worker autonomy**

Many retailers are turning to AI-trained software for workforce management. In many instances, the software is trained using datasets that are skewed or biased, and as a result the software perpetuates these institutional biases. This can lead to discrimination against workers on multiple bases, such as gender[20].

Some experts highlighted that reporting through the means of AI-enabled software removes any scope for subjective discretion that would have been exercised in exceptional cases if the worker were reporting to a human manager. For example, a worker clocking in late owing to meeting with an accident beyond their control would be excused by a manager. However, the software would recognise only that the worker had clocked in late and consequently dock / reduce pay. Experts noted that AI-enabled software also requires a certain level of technical knowledge on the part of the workers and in the absence of any effective training, leads to erroneous capture of information regarding worker productivity, which has resultant impacts on worker performance appraisal.

AI intermediation in *gig work*

- **Imposes work in poor conditions, with reduced incomes**

On-demand platforms use AI algorithms to determine a worker's aggregate rating. As the rating is linked to the income of the workers as well as the allocation of jobs to them, the opaqueness in the determination of ratings has a severely detrimental impact on the rights of the workers.

Interviews with gig workers and

[20] Dunga, C. (2020). How effective is artificial intelligence in removing racial bias in hiring?. Quartz.com. https://qz.com/work/1923587/can-artificial-intelligence-solve-racism/

experts, and existing literature showed that the opaqueness in the AI algorithmic determination of rating contributes to workers receiving inadequate income. Five gig workers we spoke to pointed out that often their rating would mysteriously drop just before the incentive was to be calculated. Similarly, some workers also noted that as they drew closer to achieving the requisite number of jobs that would qualify them for the incentive, they would get allotted fewer and fewer jobs despite no changes in rating. These experiences were corroborated by experts who either worked with gig worker unions or had conducted studies on the experiences of gig workers[21].

- **Increases risks of worker surveillance**

In order to be able to get jobs through on-demand platforms, workers are typically forced to constantly share their location data. With the onset of COVID-19, on-demand platforms started mandating that workers share sensitive personal health information, including body temperature, which is displayed to customers on the app. To ensure that they were wearing masks, the experts said, they were made to share photos of themselves through the app.

- **Leads to deprivation of social security protections**

Gig workers are classified as independent contractors. However, this classification is erroneous as the use of AI algorithms allow platform companies to dictate worker behaviour in a manner similar to an employer[22]. In many cases, workers are effectively 'locked-in' to an app as, in order to be eligible for incentives, they are forced to spend most or all of their working time with a single platform company[23]. The classification allows means that the workers are not entitled to social security protections typically afforded to employees, including health insurance, pension contribution, and paid leave.

[21] Gupta, S., & Natarajan, S. (2019). Gender and Future of Workers. Medium.com. https://medium.com/aapti/gender-and-future-of-workers-136e351266c0
[22] Siddiqui, Z., & Zhou, Y. (2021). How the platform economy sets women up to fail. Rest of World.com https://restofworld.org/2021/global-gig-workers-how-platforms-set-women-up-to-fail/
[23] PUDR. (2021). Behind the Veil of Algorithms: Invisible Workers: A Report on Workers in the 'Gig' Economy. https://pudr.org/sites/default/files/2021-12/PUDR%20report%20on%20gig%20workers-%20Behind%20the%20Veil%20of%20Algorithms.pdf

The lack of social security has a disproportionate impact on women in India, who typically work jobs which involve seasonal peak periods, and are also not eligible for maternity leave.

- **Impedes grievance redressal, leading to worker exploitation**

The lack of a legal requirement for explainable AI worsens the plight of the workers who are left in the dark regarding their ratings. Additionally, gig workers who were interviewed noted that the automated customer care mechanism, which is the first recourse available to workers, is ineffectual. Moreover, workers who fall below a particular rating are automatically locked out of the app and are required to travel to a central complaint redressal centre, which is typically a day-long affair entailing loss of pay. Some workers also reported that they had to go to these centres over a period of two to three days to have their account access restored. This was corroborated by experts, including union members and academic researchers.

Unexplainable AI, along with poor complaint redressal mechanisms, means that workers lack effective means of remedy and grievance redressal, which is accentuated by the primacy given by on-demand platforms to customers.

Role of the State in mitigating human rights risks

The following approaches may enable the Indian state to effect protection of human rights at risk from AI deployment:

- **Creating incentives for businesses to respect human rights through regulation**

The State may consider creating incentives, either through regulation or through means such as creating competition in the marketplace, which directly push businesses to adopt the human rights framing.

For instance, mandating regulatory approvals for AI technology application in the healthcare sector

pushes businesses to check for biases in their technology. In the absence of regulation, there is a certain business unwillingness to check for such biases. This measure would help in detection and mitigation of biases by businesses, preventing errors of misdiagnosis stemming from under-representation in datasets. In the financial services sector, the State can create competition regarding ensuring of privacy by setting up a framework for consumer rights and penalising businesses for data breaches. Setting up a framework of consumer rights and awareness ensures a competitive market for data where consumers avail of the service from a provider who collects less data for the same service. This is particularly important given that rampant data collection practices by businesses coupled with a lack of informed consumer consent leads to financial distress and entails exclusion harms.

In retail, the State can pass legislation requiring companies to mandatorily provide reskilling courses to employees whose jobs are affected by the adoption of AI automation. In gig work, robust regulation on having a fair contract, as well as statutory allowance for social security and minimum wages can ensure that gig workers have fair pay and social security protection.

- **Supporting businesses by establishing capacity building measures**

The State may consider capacity-building measures for businesses (technical expertise and infrastructural facilities) to support startups, which may help them in managing human rights concerns arising due to AI deployment.

Data is the input of the AI technology and the technology is as good as the data that is fed to train the algorithm. The lack of diverse datasets primarily affects data quality. India, as a low and middle income country, does face the pressing issue of lack of good quality data i.e. data which is error-free, complete and diverse. Creating datasets that are unbiased and representative in a country like India which is so vast, segregated and diverse, is a herculean task for Indian businesses currently operating in nascent stages with limited access to finance and infrastructure. In sectors of financial services and healthcare, the Government of India plays a key role in enabling availability of resources such as unbiased and

representative data fundamental to risk detection and mitigation, given its benefits from risk-free AI deployment through achievement of the broader goals of economic equality, increased access to quality healthcare and financial inclusion.

- **Ensuring enforceability of existing norms and regulations; extending applicability of laws to AI technology, wherever possible**

AI is constantly changing, though the impact on human rights of citizenry is real and on-going. The State can consider bolstering the current regulatory framework to accommodate emerging technologies like AI and mitigate their risks to human rights of citizens.

For instance, it may be beneficial to consider extending the existing RBI norms related to the right to explainability of technology to AI technology as well, in turn facilitating grievance redressal. In gig work, the Code of Social Security, 2020, is a beneficial framework stipulating worker rights. However, the State must strive to operationalise this framework of rights for AI-intermediated gig workers. Across sectors, experts believed that in the absence of privacy legislation, applicability of existing legal principles can be extended to automated decisions. For instance, the principle of 'due process' ensures that decisions affecting individuals are procedurally safeguarded against arbitrariness. Procedural safeguards include the right to the information based on which the decision was made and the right to contest the decision.

The State may additionally consider the following sector-wise mitigation strategies:

Financial Services - **Set up the regulatory framework to create an environment that increases competition to offer privacy**

Enforcement of consumer rights, stipulation of penalising regimes to curb exploitation by predatory lenders and establishment of capacity building measures for legitimate lenders to flourish are key actions for the State to undertake. Competition in offering privacy should be created from both ends – supply and demand. On the demand side, enforceability of consumer rights is key. Setting up a framework of consumer rights and

awareness ensures a competitive market for data where consumers will gravitate to the provider who collects less data for the same service. On the supply side, any breach of privacy regulation attracting penalties for a business fosters competition in offering privacy. Another form of positive reinforcement would be to directly incentivise businesses when they adhere to privacy principles according to objective norms set by the State. For instance, standardised consent makes the marketplace more competitive.

Healthcare - Strengthen regulation by stipulating liability and accountability regimes

Liability and accountability mechanisms are complex due to AI involvement in the caregiving pathway. The absence of a structured and well-defined liability and accountability regime directly affects consumer trust in the utility of AI. It is thus the primary duty of the State to stipulate frameworks of accountability defining the role, responsibility and liability of various actors involved in the caregiving pathway where AI is involved. The clinician should be made the centre of the caregiving pathway, bearing responsibility for patient care, and AI an assistive tool facilitating decision-making.

Retail - Focus on establishing capacity building measures

The State must establish capacity building measures for workers at risk of displacement and mandate effective human intervention in AI deployment. As AI deployment is expected to create millions of jobs requiring different skill sets to those possessed by workers most likely to be displaced, capacity building measures by the State can help bridge this gap and ensure displaced workers are equipped with the necessary skills to find alternative employment in an evolving economy.

Gig work - Institute a robust legal regime

The State must institute a robust legal regime that ensures adequate protection of rights of platform / gig workers. It must operationalise the legal framework for affording social security benefits as outlined in the Social Security Code, 2020, in addition to instituting data protection legislation providing workers with more rights over their data and reducing the power imbalance between platforms and workers.

Please refer to the full report for detailed action pointers or sector-wise and risk-wise mitigation strategies to be undertaken by the state.

Annexure B – Risk Assessment Toolkits

Financial Services

Actions

	Yes	No	N.A.
A. Risk to privacy			
A. 1. Adhere to minimum data collection principle			
1. Does your business adhere to the principle of minimum data collection, given that it enhances your competitive advantage?	☐	☐	☐
2. Does your business collect more data points than required?	☐	☐	☐
A. 2. Improve informed consent			
1. Does your business recognise that merely seeking consent is not adequate and that pathways to seek informed consent must be sought, i.e., ensuring that the consumer is fully aware of the nature and amount of data collected and the purposes for which it is collected?	☐	☐	☐
2. Does your business deploy specific technological tools and or other solutions that help make consumers understand consent better (for instance, nudges such as a cool-down period or visually representing privacy policies to make consumers understand privacy policies)?	☐	☐	☐
3. Does your business disclose the loan disbursement rates to allow consumers to assess the value of their data by comparing acceptance rates?	☐	☐	☐

	Yes	No	N.A.
4. Does your business collaborate with other industry members to make technological solutions that improve consent more implementable, given that they are expensive to deploy (such as deploying low-cost measures to detect and mitigate bias using natural language processing to process contracts)?	☐	☐	☐

A. 3. Seek consent for data usage

1. Does your business seek consent of the consumer prior to using data to deduce other sensitive personal information?	☐	☐	☐
2. Does your business seek consent of the consumer prior to other inferences that are drawn by the business?	☐	☐	☐

B. Risk to financial access and well-being and risk to life, dignity and safety

B. 1. Understand the context prior to deployment

1. Does your business have an AI policy to guide its use in rendering financial services?	☐	☐	☐
2. Does your business understand whether the algorithm particularly has the capability to affect particular consumer groups (positively or negatively), if inadequately or over-represented?	☐	☐	☐
3. Does your business understand the nature of algorithms being deployed in terms of potential impact on populations (that is, criticality of utility – high risk vs. low risk)?	☐	☐	☐

	Yes	No	N.A.
B. 2. Improve data representation			
1. Do you have a policy in place that mandates checking the representativeness of your dataset?	☐	☐	☐
2. Given that the standard of representativeness required varies depending on purpose of AI, is there a checklist that identifies the relevant characteristics (race, gender, etc) that a particular dataset should represent – thereby guiding the business on how to make the dataset representative and leaving out irrelevant factors/ characteristics?	☐	☐	☐
3. Are efforts taken to ensure that datasets are made representative by taking into consideration the diversity of the Indian population – race, gender, caste, urban-rural divide, etc.?	☐	☐	☐
4. Are these efforts systematically integrated into the company policy in the form of affixed pathways or SOPs?	☐	☐	☐
B. 3. Revise metrics and make it more relevant			
1. Does your business revise metrics to cater to different populations – taking into consideration digital divide and socio-economic factors that, if ignored, can amount to proxies for discrimination?	☐	☐	☐
B. 4. Initiate leadership and efforts			
1. Do you, as a business, recognise yourself as an industry giant? If yes, do you share best practices with other players to detect and mitigate bias?	☐	☐	☐

	Yes	No	N.A.
2. Do businesses collaborate with industry players to verify whether internal codes of conduct reflect principles of non-discrimination and determine reasonableness of factors or determine industry-accepted proxy factors of discrimination?	☐	☐	☐

B. 5. Improve algorithmic accuracy through testing

1. Does your business have systems in place to mitigate bias and check for algorithmic accuracy? (Measures could include testing the algorithm against different datasets and data sources, adding biased data to assess if the outcomes are biased.)	☐	☐	☐

B. 6. Improve algorithmic accuracy by measuring algorithm against outcomes

1. Does your business have any normative stipulations/ guidelines against which the outcomes can be tested?	☐	☐	☐
2. If yes, are the normative stipulations based on objective industry standards?	☐	☐	☐
3. Does your business conduct AI audits, including checking for any potential human rights risks to consumers?	☐	☐	☐
4. Are the audits conducted by independent third parties to check for biases in the outcomes based on normative stipulations?	☐	☐	☐

B. 7. Ensure human oversight

1. Is there human oversight over critical decisions – such as disbursement of loans and determination of interest rates?	☐	☐	☐

	Yes	No	N.A.
2. Does the human supervisor provide reasoned judgement as to why they concur with the decision of the AI or why the AI is justified in arriving at the decision?	☐	☐	☐
3. Are records of the aforementioned documented?	☐	☐	☐
4. Are these reasoned judgements communicated to the consumer in user-friendly simplified language?	☐	☐	☐
5. Are these decisions factored in, improving the efficacy of the AI at a later stage?	☐	☐	☐

B. 8. Focus on enhancing human resource skills

1. Does your business equip both technical and top management teams with insights on human rights risks due to use of AI tech, and its impact on diverse populations to bridge the awareness gap?	☐	☐	☐
2. Does your business equip its human resource with an understanding of the AI algorithm functioning?	☐	☐	☐
3. Was the algorithm developed by a diverse group of developers?	☐	☐	☐
4. Does your business engage with human rights expert domains like ethical data or social scientists who enable detection of proxy factors of discrimination and ascertain the reasonableness of factors or meaningful correlation between creditworthiness and the factor for ascertaining creditworthiness?	☐	☐	☐

B. 9. Establish accountability mechanisms

1. Does your business build internal capacity to understand algorithmic programming?	☐	☐	☐

	Yes	No	N.A.
2. Does your business keep track of the characteristics of datasets used to train the algorithm (example – does the business document which metrics were considered as relevant and the underlying reason, the sources of their input data, and the reasons for denial of loan. what were the criteria to decide what dataset should be selected and why?)?	☐	☐	☐
3. Does your business document potential sources of bias or entry points?	☐	☐	☐

B. 10. Continue R&D phase until scale-up phase

1. Does your business retrain the algorithm on revised datasets periodically to account for changing demographics in order to ensure accuracy of the AI?	☐	☐	☐

B. 11. Represent product and its limitation

1. Does your business provide the following information to consumers *a. AI system's capabilities and limitations,* *b. the purpose for which the systems are intended,* *c. the conditions under which they can be expected to function as intended and* *d. the expected level of accuracy in achieving the specified purpose?*	☐	☐	☐
2. Is the information so provided concise and easily understandable?	☐	☐	☐

	Yes	No	N.A.
B.12 Differentiate business from predatory lenders			
1. Does your business make efforts to differentiate itself from predatory lenders through legal (e.g. non-predatory lenders should regularly conduct due diligence for copyright infringement and sue predatory lenders for copyright infringement of their domain names) and non-legal means (e.g. publication in the newspapers to make consumers aware)?	☐	☐	☐

C. Risk to effective remedy and grievance redressal

C. 1. Afford the right to know reason for credit denial			
1. Does your business provide a reasoned judgement as to why a consumer was denied credit?	☐	☐	☐
2. Does your business disclose key factors that affect the score or creditworthiness? Based on the order of importance, the business can disclose at least the top three reasons or factors that were relied on to determine creditworthiness.	☐	☐	☐
3. Has your business set up in-house grievance redressal mechanism as the first point of escalation (for instance, chatbots on consumer facing digital lending apps)?	☐	☐	☐
4. Does your business have established grievance redressal channels for consumers to challenge/ appeal a decision taken on their applications?	☐	☐	☐
5. Does your business lay out various options for remedy and redressal available (judicial and non-judicial) for consumers to resort to in the event they are not satisfied with the in-house redressal?	☐	☐	☐

	Yes	No	N.A.
C. 2. Create feedback mechanisms			
1. Does your business include consumers who have complained or consider themselves targets of bias/ discrimination included in the review process of the algorithm?	☐	☐	☐
2. Does your business provide opportunity to rectify data of consumers if consumers identify that loan has been denied based on inaccurate data?	☐	☐	☐
3. Does your business document all reasons for loan denial and subsequent objections raised by consumers against algorithmic decisions as they will help to detect biases if loans are consistently denied to persons belonging to a particular group?	☐	☐	☐
C. 3. Focus on making AI explainable			
1. Does your business make efforts to make AI as explainable as possible?	☐	☐	☐
2. Does your business have an internal policy that guides responsible procurement of AI technology? (Responsible procurement policy should ensure that AI procured is explainable and transparent.)	☐	☐	☐

Healthcare

Actions

	Yes	No	N.A.
A. Likelihood of bias and discrimination			
A. 1. Understand the context prior to deployment			
1. Does your business have an AI policy in place to guide development of the algorithm?	☐	☐	☐
2. Does your business understand whether the algorithm particularly has the capability to affect particular patient groups (positively or negatively), if they are inadequately or over-represented in the data pool?	☐	☐	☐
3. Does your business understand the nature of the algorithm being deployed in terms of its potential impact on populations (that is, criticality of its utility – high risk vs. low risk)?	☐	☐	☐
A. 2. Improving algorithmic accuracy by enhancing input data quality			
a. How representative is your dataset?			
1. Do you have a policy in place that mandates periodically checking the representativeness of your dataset?	☐	☐	☐
2. Given that the standard of representativeness required varies depending on purpose of AI, is there a checklist that identifies the relevant characteristics (race, gender, etc) that a particular dataset should represent – thereby guiding the business on how to make the dataset representative, leaving out irrelevant factors/characteristics?	☐	☐	☐

	Yes	No	N.A.
3. Are efforts made to ensure that datasets are made representative by taking into consideration the diversity of the Indian population – race, gender, caste, urban-rural divide, etc.?	☐	☐	☐
4. Are these efforts systematically and periodically integrated into the policy in the form of affixed pathways or SOPs?	☐	☐	☐
5. Is there any training afforded to required employees/AI developers to create awareness and check for these inconsistencies periodically?	☐	☐	☐
b. How error-free is your data?			
1. Does your business provide opportunities to consumers to correct or rectify their data periodically in order to ensure that datasets are accurate?	☐	☐	☐
A. 3. Improve algorithmic accuracy through testing			
1. Does your business have systems in place to mitigate bias and check for algorithmic accuracy? (Measures could include testing the algorithm against different datasets and data sources, and adding biased data to assess if the outcomes are biased.)	☐	☐	☐
A. 4. Improve algorithmic accuracy by measuring algorithm against outcomes			
1. Does your business have any normative stipulations/ guidelines against which the outcomes can be tested?	☐	☐	☐
2. If yes, are the normative stipulations based on objective industry standards?	☐	☐	☐

	Yes	No	N.A.
3. Does your business conduct AI audits, including checking for any potential human rights risks to patients?	☐	☐	☐
4. Are the audits conducted by independent third parties to check for biases in the outcomes, based on normative stipulations?	☐	☐	☐

A. 5. Focus on enhancing human resource skills

1. Does your business equip both technical and top management teams with insights on human rights risks, and its impact on diverse populations to bridge the awareness gap?	☐	☐	☐
2. Does your business equip its human resource with an understanding of the AI algorithm functioning?	☐	☐	☐
3. Was the algorithm developed by a diverse group of developers?	☐	☐	☐
4. Does your business engage with human rights expert domains like ethical data or social scientists who enable detection of sources of bias and ways to mitigate them, and have the capability to integrate ethics into design?	☐	☐	☐
5. Does your business engage with experts in medical knowledge like clinicians who enable detection of sources specific biases likely to occur in the field of medicine and medical data?	☐	☐	☐

A. 6. Establish accountability mechanisms

1. Does your business build internal capacity to understand algorithmic programming?	☐	☐	☐

	Yes	No	N.A.
2. Does your business keep track of the characteristics of datasets used to train the algorithm (example – what were the criteria to decide what dataset should be selected and why?)?	☐	☐	☐
3. Does your business document potential sources of bias or entry points?	☐	☐	☐

A. 7. Continue R&D phase until scale-up phase

1. Does your business retrain the algorithm on revised datasets periodically to account for changing demographics in order to ensure accuracy of the AI?	☐	☐	☐

A. 8. Represent product and its limitation

1. Does your business provide the following information to consumers (clinicians) – AI system's capabilities and limitations, the purpose for which the systems are intended, the conditions under which they can be expected to function as intended and the expected level of accuracy in achieving the specified purpose?	☐	☐	☐
2. Is the information so provided concise and easily understandable?	☐	☐	☐
3. Does your business consider constructing a separate model where the results of accuracy are low for a particular group?	☐	☐	☐

	Yes	No	N.A.

B. Loss of individual autonomy (doctor and patient)

B. 1. Focus on clinician understanding of AI

1. Does your business ensure that the clinician has a reasonable understanding of the working of the AI, sufficient for them to understand and explain to patients how the AI reached a particular decision?	☐	☐	☐
2. Does your business provide user training, covering how the AI model works in the overall system, how to use the insights it generates, and how/when to override its outputs, systematically developed, delivered, and documented?	☐	☐	☐
3. Are communication protocols established that fulfill minimum standards of detail equivalent to clinician to clinician handoff?	☐	☐	☐
4. Does your business have an internal policy that guides responsible procurement of AI technology? (Responsible procurement policy should ensure that AI procured is explainable and transparent.)	☐	☐	☐

B. 2. Maintain oversight by clinician/supervision by clinician

1. Is the clinician made aware of his role as a mediator between the AI and the patient to initiate transparency, making AI explainable which is critical to patient autonomy?	☐	☐	☐
2. Is the clinician made aware of the communication protocols with patients which are based on choice architecture frameworks, strengthening patient autonomy (example – each decision predicted will correspond to a risk score)?	☐	☐	☐

	Yes	No	N.A.
3. Is the clinician instructed to keep track of their decisions that are facilitated by the AI in critical care – justifying why they preferred to access/deviate from the suggestion made by the AI?	☐	☐	☐
4. Is any decision by the clinician to deviate from the AI factored into the testing/upgrading of algorithm at a later stage?	☐	☐	☐
5. Does your business develop mechanisms in AI deployment that allow interventions by clinicians (e.g. in consumer facing apps, businesses should develop AI in a way so that it suggests intervention by a medical healthcare professional when it is of the opinion that the problem is beyond its expertise)?	☐	☐	☐

B. 3. Create patient feedback loops/protocols

1. Does your business (healthcare providers) have systems in place to receive patient feedback – channels to understand and address patient concerns and grievances?	☐	☐	☐
2. Does your business include consumers who have complained or consider themselves targets of bias/ discrimination included in the review process of the algorithm?	☐	☐	☐

B. 4. Communicate with affected stakeholders and other stakeholders

1. Does your business actively make the public aware of the possible risks of AI in predictive healthcare, and identification and mitigation?	☐	☐	☐

	Yes	No	N.A.

C. Loss of data privacy

C. 1. Healthcare provider must inform patients of AI usage

1. Does the healthcare provider inform patients of AI usage and its involvement in facilitating decision-making? ☐ ☐ ☐

C. 2. Simplify data collection, storage and usage practices and processes for customers

1. Are you making available the utility and intended purpose of AI-based predictive analytics to patients in easy to understand material? ☐ ☐ ☐

2. Does your business seek consent continuously for all the data points collected during continuous monitoring of patient behaviour, data usage and inferences made? ☐ ☐ ☐

3. Does your business adopt a privacy by design approach (particularly relevant for consumer facing apps, which must collect minimum personal data and anonymise data, wherever reasonably possible)? ☐ ☐ ☐

C.3. Initiate leadership and efforts

1. Do you, as a business, recognise yourself as an industry giant? If yes, do you share industry best practices with other players to detect and mitigate risks? ☐ ☐ ☐

2. Does your business collaborate with other industry members to make technological solutions that improve consent more implementable, given that they are expensive to deploy? ☐ ☐ ☐

Retail

Actions

	Yes	No	N.A.
A. Loss of jobs			
A. 1. Identification of sites of automation			
1. Does your business conduct planning surveys to identify sites within the business that are most conducive to AI-enabled automation?	☐	☐	☐
2. If yes, does this survey include metrics on how many jobs will be displaced as a result of AI-enabled automation?	☐	☐	☐
3. Does your business take into account the new skills that will be required from the workforce as a result of AI-enabled automation?	☐	☐	☐
A. 2. Assessment of feasibility of reskilling initiative			
1. When looking at the new skills required owing to automation deployment, is there an assessment of the competencies of existing workers?	☐	☐	☐
2. In making the decision to conduct (or not conduct) reskilling initiatives, are the following metrics taken into consideration?			
a. Long-term (>4 years) financial gains to the organisation	☐	☐	☐
b. Availability of competent external personnel	☐	☐	☐
c. Retention of institutional capacity	☐	☐	☐
d. Downtime from onboarding new resources	☐	☐	☐
e. Goodwill from customers and employees	☐	☐	☐

	Yes	No	N.A.
3. Are workers' opinions regarding reskilling initiatives considered when making the assessment?	☐	☐	☐

A. 3. Reskilling of workers

1. Are existing workers considered by management for reskilling when automation is being implemented?	☐	☐	☐
2. If yes, are the metrics used to determine which workers are selected fair, transparent and free of bias?	☐	☐	☐
3. Are existing workers consulted on whether they would like to participate in reskilling efforts?	☐	☐	☐
4. Is accurate and complete information provided to workers on the nature of the new skills required, a description of the new job they will perform post-reskilling, and the likely pros and cons of choosing to reskill or not?	☐	☐	☐
5. Are workers who choose to not reskill provided any form of compensation or severance package?	☐	☐	☐

A. 4. Post automation integration

1. Do you provide adequate support and training to reskilled workers once they are placed in new roles?	☐	☐	☐
2. Is worker feedback taken into account in fine tuning and adjusting the deployment of automation?	☐	☐	☐

	Yes	No	N.A.
B. Erosion of worker autonomy + risk of discrimination			
B. 1. Understand the context prior to deployment			
1. Does your business understand whether the AI workforce management system has the capability to affect particular worker groups (positively or negatively), if inadequately or over-represented?	☐	☐	☐
B. 2. Improve data representation			
1. Do you have a policy in place that mandates checking the representativeness of the dataset on which the AI system is trained?	☐	☐	☐
2. Are efforts taken to ensure that datasets are made representative by taking into consideration the diversity of the Indian population – race, gender, caste, urban-rural divide, etc.?	☐	☐	☐
3. Are these efforts systematically integrated into the policy in the form of affixed pathways or SOPs?	☐	☐	☐
B. 3. Initiate leadership and efforts			
1. Do you, as a business, recognise yourself as an industry giant? If yes, do you share best practices with other players to detect and mitigate bias?	☐	☐	☐
2. Do businesses collaborate with industry players to verify whether internal codes of conduct reflect principles of non-discrimination and determine reasonableness of factors or determine industry-accepted proxy factors of discrimination?	☐	☐	☐

	Yes	No	N.A.
B. 4. Improve accuracy by measuring AI system against outcomes			
1. Does your business have any normative stipulations/guidelines against which the outcomes can be tested?	☐	☐	☐
2. If yes, are the normative stipulations based on objective industry standards?	☐	☐	☐
3. Does your business conduct AI due diligence, including checking for any potential human rights risks to worker interests?	☐	☐	☐
4. If yes, are these audits done by independent third parties to check for biases in the outcomes based on normative stipulations?	☐	☐	☐
B. 5. Ensure human oversight			
1. Is there regular human oversight over critical decisions – such as calculation of income?	☐	☐	☐
2. Does the human supervisor provide a reasoned judgement as to why they concur with the decision of the AI system?	☐	☐	☐
3. Are records of the aforementioned documented?	☐	☐	☐
4. Are these reasoned judgements communicated to the worker in user-friendly simplified language?	☐	☐	☐
5. Is there periodic human oversight of the accurate working of the AI system, including accounting for any deviations from AI analysis, to improve AI systems?	☐	☐	☐

	Yes	No	N.A.
6. Does your business have an internal policy that guides responsible procurement of AI technology? (Responsible procurement policy should ensure that AI procured is explainable and transparent.)	☐	☐	☐

B. 6. Focus on enhancing human resource skills

1. Does your business equip both technical and top management teams with insights on human rights risks, and the impact on diverse populations to bridge the awareness gap?	☐	☐	☐

B. 7. Adequate redressal mechanisms

1. Does your business provide workers with an adequate, accessible and effective grievance redressal mechanism to correct errors in the functioning of the system?	☐	☐	☐
2. Does the grievance redressal mechanism involve human management personnel?	☐	☐	☐
3. Does the grievance redressal mechanism allow for the correction of erroneously captured data?	☐	☐	☐

B. 8. Iterative refinement of the AI system

1. Does the business consult with the external software provider to have the system refined based on working observations?	☐	☐	☐
2. Is worker feedback incorporated into refinement of the AI system?	☐	☐	☐
3. Is worker feedback accurately relayed to the external software provider?	☐	☐	☐

Gig Work

Actions

	Yes	No	N.A.
A. Inadequacy of Income + poor working conditions			
A. 1. Income determination			
1. Does the incentive structure for workers provide them an adequate level of income?	☐	☐	☐
2. In order to be eligible for the incentives, do workers have to spend most of their time on the business's platform, in contravention of the promise of 'flexible work' by the platform?	☐	☐	☐
3. Is the incentive structure clearly explained to the workers?	☐	☐	☐
4. Is the incentive structure, including how the factors responsible for calculating the incentives and their weightage, listed in the contract with the worker?	☐	☐	☐
A. 2. Safe and healthy working conditions			
1. Does the business engage with workers periodically to understand their working conditions?	☐	☐	☐
2. Does the business engage with workers periodically to understand changes that they would like to be implemented to improve working conditions?	☐	☐	☐
3. Does the business ensure safe and healthy working conditions for the workers?	☐	☐	☐

	Yes	No	N.A.
4. Is any measure taken to interact with other partners that the worker might interface with, to ensure that the worker is given basic safety and access to basic necessities? (For example, access to washroom facilities at partner restaurants.)	☐	☐	☐
5. Are extra steps taken to ensure the safety of women workers?	☐	☐	☐
6. Is there an accessible helpline operated by human personnel for workers to contact in case of an emergency or safety concern?	☐	☐	☐

A. 3. Rating determination

1. Are the workers made aware of the criteria that go into determining their rating, along with the weightage for each factor?	☐	☐	☐
2. Are workers given the right to challenge the rating determined by the algorithm?	☐	☐	☐
3. Does a challenge by the worker result in an investigation into the decision made by the algorithm in determining the rating?	☐	☐	☐
4. Are workers able to challenge the rating given to them by a customer?	☐	☐	☐
5. Can the rating given by a customer be revised subsequent to a review process on a challenge by the worker?	☐	☐	☐

	Yes	No	N.A.
A. 4. Oversight of functioning of the algorithm			
1. Are periodic checks performed on the functioning of the algorithm to ensure its accurate and non-biased functioning?	☐	☐	☐
2. Is the algorithm audited by an independent third party for fairness and bias?	☐	☐	☐
3. Is the algorithm designed taking into account the vulnerabilities of different groups (platform workers), so as to ensure that certain groups are not disadvantaged? (For example, women are also burdened with household responsibilities and are not able to give as much time as men might, or take advantage of 'peak hour' rates.)	☐	☐	☐
A. 5. Initiate leadership and efforts			
1. Do you, as a business, recognise yourself as an industry giant? If yes, do you share best practices with other players to detect and mitigate bias?	☐	☐	☐
2. Do businesses collaborate with industry players to verify whether internal codes of conduct reflect principles of non-discrimination and determine reasonableness of factors or determine industry-accepted proxy factors of discrimination?	☐	☐	☐

B. Worker Surveillance

B. 1. Adhere to minimum data collection principle			
1. Does the business collect more than the minimum amount of data required to enable workers to work on the platform?	☐	☐	☐

	Yes	No	N.A.
B. 2. Improve informed consent			
1. Does the business recognise that merely seeking consent is not adequate and that pathways to seek informed consent must be sought?	☐	☐	☐
2. Does the business deploy specific technological tools and solutions that help improve consent?	☐	☐	☐
3. Does the business engage with workers to check if they understand the implications of the provisions they are consenting to?	☐	☐	☐
4. Does the business collaborate with other industry members to make technological solutions that make consent better?	☐	☐	☐
B. 3. Seek consent for data usage			
1. Does your business seek consent of the worker prior to processing their data?	☐	☐	☐
2. Does the consent sought for processing the data of the worker include consent for the possible consequences of such processing?	☐	☐	☐
3. Does the business seek consent from the worker for sharing the data of the worker with third parties?	☐	☐	☐
4. Are workers made aware of who their data is being shared with?	☐	☐	☐
5. Are workers given the choice to ensure their data is not shared with third parties to the extent that such sharing is not essential for providing services on the platform?	☐	☐	☐

	Yes	No	N.A.
6. Is the collection and processing of workers' data in compliance with extant legal provisions?	☐	☐	☐

C. Absence of Social Security

C. 1. Worker-business relationship

1. Does the business have the ability to exert significant influence over the actions of the worker? For example, does the business have the ability (through the use of ratings and incentive structures) to influence how many platforms the worker performs tasks on?	☐	☐	☐
2. Does the business constantly monitor the performance of the worker?	☐	☐	☐
3. Is the effective power dynamic between the business and the worker such that the worker's independence is negated?	☐	☐	☐
4. Does the business engage with workers to understand how they view the business in terms of employment?	☐	☐	☐

C. 2. Social security measures

1. Does the business provide any social security to the workers, e.g. health and accident insurance, etc.?	☐	☐	☐
2. Does the business provide a guaranteed basic wage to workers?	☐	☐	☐
3. Are workers given a quantum of paid leave in consonance with labour laws applicable to employees?	☐	☐	☐
4. Is the business in compliance with extant legal provisions on social security measures for platform workers?	☐	☐	☐

	Yes	No	N.A.
5. Does the business engage with workers to understand their needs?	☐	☐	☐
6. Does the business implement measures from a social security perspective to address these needs?	☐	☐	☐

D. Risk to effective remedy and grievance redressal

D. 1. Afford the right to know reason for reduction in rating or blocking from the app

1. Does the business have an established accessible and effective grievance redressal mechanism for workers?	☐	☐	☐
2. Does the business provide a reasoned explanation as to why the worker's rating was decreased?	☐	☐	☐
3. Does the business provide a reasoned explanation as to why the worker was locked out of the platform (outside of the worker's rating falling below the predetermined threshold)?	☐	☐	☐
4. Does the business disclose to the worker the criteria that affect his/her ratings?	☐	☐	☐

D. 2. Create feedback mechanisms

1. Does the business engage with workers to understand their problems with the algorithmic determination of ratings?	☐	☐	☐
2. Is feedback from the workers incorporated into revising the algorithm to remove bias and discrimination?	☐	☐	☐

	Yes	No	N.A.
3. Does the business's internal company policy prioritise worker safety and health?	☐	☐	☐

D. 3. Focus on making AI explainable

1. Does the business make efforts to make the algorithm as explainable as possible to workers?	☐	☐	☐
2. Does the business have an internal policy that guides responsible development and procurement of AI technology? (Such a policy should ensure that AI developed or procured is explainable and transparent.)	☐	☐	☐

Annexure C – List of Experts

Financial services

Name	Affiliation	Designation
Natalia	Zest Money	Lead, AI
Ankita Singh	UNCDF	Financial Health Advisor
Jaspreet Singh	UNCDF	Global Lead, Financial Health and Innovations
Beni Chugh	Dvara Research	Research Manager
Rahul Matthan	Trilegal	Partner
Vinay Kesari	Setu	General Counsel
Suchita	Light Rock	General Counsel
Tarunima Prabhakar	Carnegie India	Non-Resident Fellow
Rohin Garg	IFF	Policy Counsel
Priyashmita Guha	DLAI	Director
Jayashree Venkatesan	Centre for Financial Inclusion	Director
Sandeep Farais	Elevar Equity	Founder and Managing Partner
Alex Rizzi	Centre for Financial Inclusion	Senior Director
Preeti Syal	NITI Aayog	Technologist

Healthcare

Name	Affiliation	Designation
Tejasvi Ravi	Light Rock	Health Investor
Abhishek Jain	Swasth	CTO
Lavanya Bhamidipati	In Health Ventures	Digital Health Investor
Praful Krishna	HealthIQ	VP Product Management
Suchita	Light Rock	General Counsel
Mrinal Sinha	Vitraya Tech	CEO & Co-Founder
Rahul Matthan	Trilegal	Partner
Sandeep Farais	Elevar Equity	Founder and Managing Partner
Preeti Syal	NITI Aayog	Technologist

Retail

Name	Affiliation	Designation
Mayank Tiwari	Avataar.me	Partner & CBO
Krish Sridhar	KNOW App	Founder & CEO
Vinay Joy	Khaitan & Co.	Partner
Aditi Surie	Indian Institute of Human Settlements	Consultant
Akshay Kharbanda	*(confidential on request)*	Public Policy & Regulatory Affairs
Preeti Syal	NITI Aayog	Technologist

Gig Work

Name	Affiliation	Designation
Aditi Surie	Indian Institute for Human Setllements	Consultant
Aayush Rathi	Centre for Internet and Society	Senior Researcher
Girish R.	Ola	Driver Partner
Sarthak K.	Uber	Driver Partner
Mallesh G.	Uber	Driver Partner
Salman Md.	Urban Company	Partner
Bhupesh Kumar	Zomato	Rider Partner
Birappa Hanamantha	Swiggy	Rider Partner
Jai Vipra	All India IT and ITes Employees' Union	
Shruti Gupta	National University of Singapore	PhD Researcher
Preeti Syal	NITI Aayog	Technologist

aapti institute 2022

Aapti is a public research institute that works at the intersection of technology and society. It examines the ways in which people interact and negotiate with technology both offline and online.

contact@aapti.in

www.aapti.in | www.thedataeconomylab.com

aapti institute

Funded by the European Union

B+HR BUSINESS AND HUMAN RIGHTS | ASIA

UNDP