UK INDIA
BUSINESS COUNCIL

DATA: THE FOUNDATION OF INTELLIGENT ECONOMIES

INDIA'S DATA PROTECTION AND THE FUTURE OF THE UK-INDIA TECH PARTNERSHIP

MARCH 2019

CONTENTS

FOREWORD

Data has become one of the most precious, and discussed, commodities of the 21st century. It has the power to improve access to services across the social spectrum and is becoming a primary source of wealth generation as it creates new paradigms of business activity. And yet, data, or the misuse of data, has also given rise to equally animated discussion on access, ownership, and consent.

Globally, the major governmental stakeholders in the new digitisation revolution are rolling out Data Protection legislation. Yet, there is no consensus as to how this should be done and the implications of this inconsistency will have profound implications in the near future.

Following the publication of India's draft Personal Data Protection Bill 2018, this report represents our contribution to the debate as the voice of businesses in the UK-India corridor. Certain observations notwithstanding, the UK India Business Council (UKIBC) gives a cautious welcome to India's balanced qualified-consent, qualified-access approach. We examine the opportunities presented by India's rise as a data super-power and, specifically, the opportunities for greater and mutually beneficial collaboration between UK and Indian businesses.

Both Governments see the role of the State as that of an enabler, and both see their AI strategies as being ethical and orientated towards solving socio-economic problems. At the same time, there is complementarity and familiarity between key UK and Indian companies which is underpinned by existing vibrant research.

UKIBC believes that the UK-India Tech Partnership, announced in April 2018 by Prime Ministers May and Modi, is a good starting point for this collaboration. While many initiatives have already taken place, we would encourage greater urgency. Specifically, business-led initiatives could be used to develop AI technologies across the five priority sectors identified in NITI Aayog's National Data Strategy published last year.

As such, UKIBC urges the UK and Indian Governments to create a business-led 'Data Garage' under the UK-India Tech Partnership. This 'Data Garage' would explore AI and associated technologies on a controlled 'open-source' basis via 'sandbox' protocols, link to the proposed 'National Centre for Artificial Intelligence', and work closely with a network of Centres of Research Excellence (COREs) and their UK counterparts.

We would like to thank all the businesses and industry experts - both Indian and UK - who have taken the time to review, discuss, and share their insights on the themes of this report. Our gratitude also extends to the Pahle India Foundation, our research partners investigating the Bill's proposed provisions, and to the Department for International Trade (DIT) for facilitating the India-UK FutureTech Festival in December 2018, at which we hosted a televised panel discussion on AI and data protection.

I hope you enjoy the report and find it a compelling read.

Richard Heald, OBE
Group CEO, UK India Business Council

INTRODUCTION

India is on the cusp of implementing legislation that will govern the use of immense personal data caches being generated by nearly a fifth of the world's population.

With the delivery of the JAM (Jan Dhan-Aadhaar-Mobile) trinity, the implementation of the Goods and Services Tax (GST), online filing of taxes, and the explosion of social media and online shopping, India potentially holds the largest personal data-cache in the world. And this is growing. Exponentially.

Personal data is the lifeblood of innovation, AI, and business in the 21st century. India's steps to protect and regulate personal data protection is therefore timely. The approach that is adopted, however, is critical as it is not hyperbole to say that India's Personal Data Protection Bill will have profound consequences for Indian and global stakeholders.

India's ability to minimise data misuse and maximise its immense data opportunity in an innovation-friendly framework, would pave the way for revolutionising Indian livelihoods, from meaningful access to healthcare and education, to having real retail choice and financial independence.

At the same time, India rightly has the ambition to be the go-to data solutions hub for developing countries across 40% of the world solving the largest socio-economic problems plaguing our societies. Though the scale of India's data wealth and AI absorption gives a promising foundation for achieving this, it will not be enough in and off itself. Collaborations in tech-trade and digital innovation, particularly in the roll-out of AI, will be crucial.

The UK is a world-leader in AI research and innovation, with the resource, finance, and expertise to help deliver India's AI and data ambitions. There are immense complementarities between UK and Indian digital business capabilities that if enabled, we believe, could see both countries pioneer the fourth industrial revolution together.

Unlocking this would take an ambitious agreement to the shared transfer and processing of data between our two countries. This is why, in this report, the UKIBC is urging both Governments to expand the scope of the UK-India Tech Partnership and prioritise the formation of pioneering business-led collaborations focusing on the five key areas highlighted by NITI Aayog in their National Data Strategy report.

In summary, the UKIBC welcomes India's overall framework based on a balanced "qualified consent, qualified access" regime. Subject to further consultation and clarity on key provisions for data localisation, the independence, effectiveness, and funding of the regulator, and appropriate dispute resolution mechanisms, UK and Indian businesses are keen that both Governments develop the UK-India Tech Partnership in a way which grasps the biggest ease of doing business reform of the 21st century.

1.1 OUTLINE OF THE REPORT

This report makes the case for a liberal, transparent, and fair approach to personal data protection regulation in India, paving the way for prioritising a Common Data Agreement (CDA) within the UK-India Tech Partnership.

In making this case, we first outline the value of personal data to 21st century business and tech-trade before laying bare the UK and India's complementary AI and data strengths and ambitions.

This could not be more stark in the field of healthcare AI, where the introduction of the Ayushman Bharat healthcare insurance scheme will require pioneering AI expertise and collaboration to be achieved.

This lays the foundation in making our case for a joint virtual 'Data Garage' facilitated by a UK and India Common Data Agreement (CDA) at the end of section 3. A prerequisite to forming a CDA, however, is ensuring adequate protection and safeguards are in place for the use and transfer of personal data in India. Indeed, this is increasingly an unignorable starting point for businesses regardless.

This leads us to investigate and summarise the main provisions of India's draft Personal Data Protection Bill 2018 which we then evaluate against the needs of business, and subsequently, against the requirements needed to make a CDA possible.

In doing so, we acknowledge cautiously that the proposed Bill strikes a potentially innovative and business-friendly framework that could very much facilitate a CDA subject to the important clarifications we have outlined in the recommendations of this report

2. THE IMPORTANCE OF DATA TO BUSINESS AND INTERNATIONAL TRADE

"Data are (sic) to this century what oil was to the last one: a driver of growth and change. Flows of data have created new infrastructure, new businesses, new monopolies, new politics and - crucially - new economics."[1]

The difference between artificial intelligence (AI) and technology is data. Where technology carries out a set task in a pre-programmed way, AI uses relevant data inputs to improve and adapt its approach to carrying out the task. Generally, more data leads to better AI outcomes, and hence 'Big Data' carries the potential to revolutionise technology, the economy and society.

2.1 WHAT DATA?

Data has already become such a pervasive, though accepted, part of our lives and work that its impact has evolved beyond its use in computing applications. Data, in the digital context, is information that has been transformed into a format easy and efficient to move, process, and analyse en masse.

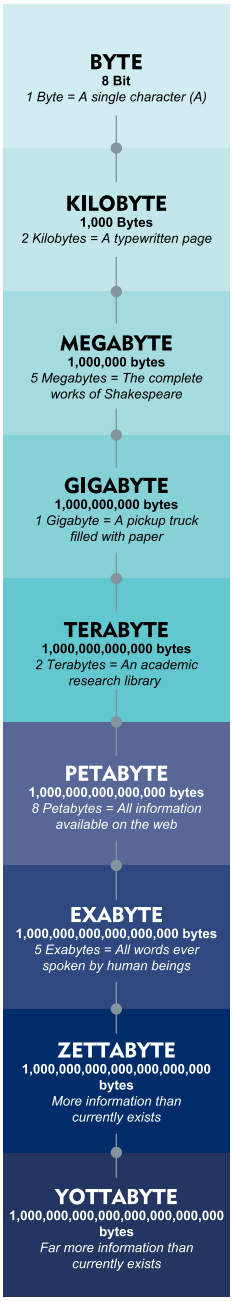
This can be information relating to an identifiable individual (such as what car they drive), in which case it is personal data, information relating to a machine process or product (performance of a car component when tested), in which case it is machine generated data, or information relating to a business and its operations (such as sells of a car), in which case it is business data.

Information relating to an identifiable individuals experience of a process, use of product, or engagement with a business (where a person buys their car or drives their car) is treated as personal data.

In its simplest form, data is translated into a series of raw, binary 0's and 1's stringed together in chains from a single byte to ig Data often stored mega and gigabytes. The mass roll out of the internet, computers, and smartphones (vz the Jan Dhan - Aadhar - Mobile trilogy in India) transforming our lives, work, and business has resulted an the enormous growth of data on all fronts. Digital data now spans almost any format on a scale that the term 'Big Data' barely captures.

Today the digital universe doubles every two years. This represents a 50-fold growth in data from 2010 to 2020 alone. Personal and machine data is experiencing an overall 10 times faster growth rate than traditional business data, and machine data is increasing even more rapidly at 50 times the growth rate.[2]

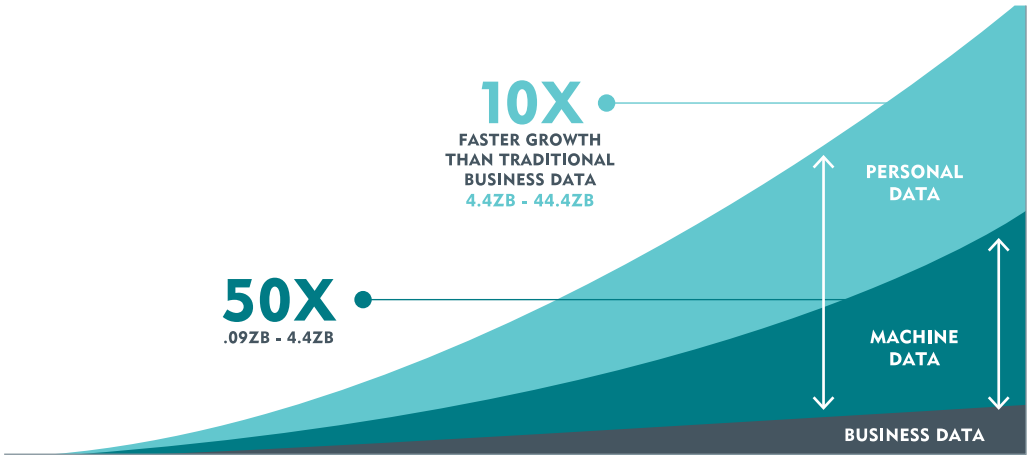
A BIT OF BYTES



Sources

1. The Economist, 'The Worlds Most Valuable Resource', 6th May 2017
2. InsideBIGDATA, "Guide to Use of Big Data on an Industrial Scale", 2017

GRAPH 1 - GROWTH IN PERSONAL, MACHINE, AND BUSINESS GENERATED DATA



2.2 MODERN DATA ARCHITECTURE

In the first Industrial Revolution, the Spinning Jenny's all-important punch card stored data measured in bits. Since then, the exponential growth and proliferation of data has led to significantly enhanced storage capacity and sophistication.

Commercial users ideally aim to access both 'raw' and 'metadata' in large data-sets they can move without need to re-configure the data. Yet, whilst the level of innovation has been immense, physical (and virtual) servers remain central to modern data architecture and important in understanding the movement of data and data localisation

The Cloud (see Glossary) is the current go-to medium of data storage allowing users to access data via physical or virtual servers maintained by a cloud service provider such as Amazon Web Services, Azure, Google Cloud, or Snowflake.

Within the Cloud exist platforms such as Data Lakes and Data Warehouses. These systems are both widely used for storing Big Data, but they are not interchangeable infrastructure. The former is a vast pool of raw data, the purpose for which is not yet defined and often facilitates large 'Data Garages', while a Data Warehouse is a repository for structured, filtered data that has already been processed for a specific purpose.

As Talend, a Cloud Data Integration business, notes, there are several important differences between a Data Lake and a Data Warehouse based on data structure, ideal users, processing methods, and the overall purpose of the data as outlined in Table 1.

TABLE 1 - DISTINGUISHING BETWEEN DATA LAKES AND WAREHOUSES

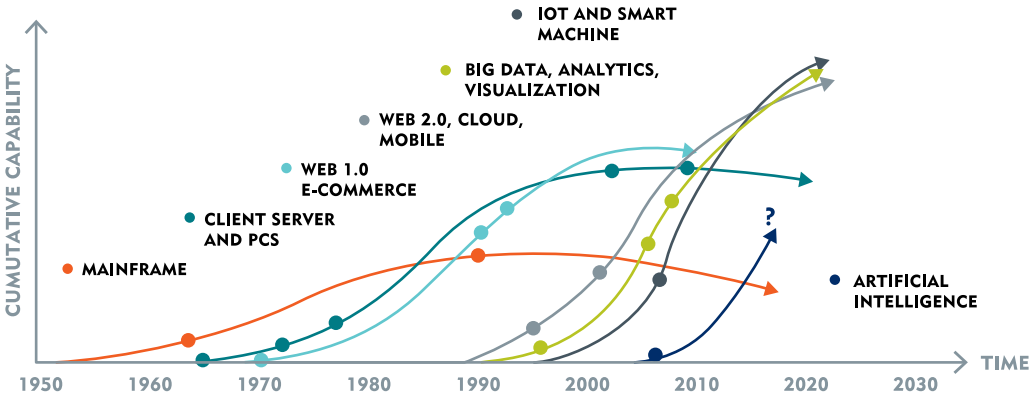
	DATA LAKE	DATA WAREHOUSE
DATA STRUCTURE	Single source of all enterprise data including 'raw' data	Processed data from many sources
PURPOSE OF DATA	Not yet determined	Currently in use
USERS	Data scientists	Business professionals
ACCESSIBILITY	Highly accessible and quick to update	More complicated and costly to make changes

Key to determining how, when and where data storage is used is the commercial facilitation and cost. As the R&D spend of companies rises, many are increasingly operating an IT strategy of "twice the value at half the cost".[3] As such, predominantly large and multinational organisations with access to economies of scale that develop Data Lakes, with smaller businesses tending to rely on Data Warehouses and open-source data.

AstraZeneca estimates that its total data in-house storage amounts to 20,000 Terabytes and that with their current research focus on genomics will generate a further 1,000 Terabytes of Data per annum. Data agility and the ability to precisely deliver the right data sets to the right place in the right format are key to continued innovation.

Thus ensuring that Data Lake platforms, such as those managed by Azure, are open and flexible is crucial to allowing data to be seamlessly managed across both applications and a global network of Microsoft managed data centres.

GRAPH 2 - INCREASING RATE OF TECHNOLOGY INNOVATION



Based on work by Publicis .Sapient, 2019

Sources

3. Diginomica, "AstraZeneca reveals the data engine behind their cloudy business transformation", 2018

This flexibility, aggregation, and cost advantage afforded by data storage infrastructure are a key determinant in businesses being able to drive innovation and deliver consumer value.

As Graph 2 demonstrates, the rate of technology innovation is accelerating with the rise of AI, IoT (see Glossary), and smart machines etc. This drives the improvement of existing data architecture or displaces outdated technologies that cannot keep up.

It comes as no surprise, therefore, that businesses are already thinking beyond the potential of cloud storage. For instance, highly anticipated research into 'hologram technology' indicates it will require only a single centimetre to store 1 Terabyte, and less than 10 centimetres to store the capacity of a human brain.[4]

2.3 THE VALUE OF DATA TO BUSINESS

AI, machine learning, and future technology accesses large volumes of "raw" data, which algorithms and application programming interfaces (APIs - see Glossary) use to yield predictions, identify trends, and learn how to carry out tasks whether supervised or unsupervised.

Realising this potential value from AI rests on the relationship between data and machine learning. Given the immense growth in personal and machine data relative to business data - these two areas represent where AI will deliver the greatest value for businesses.

In the report 'Big Data in Big Companies', IIA Director, Tom Davenport, describes three key ways in which businesses derive value from AI[5]:

1. **Cost reduction.** Big Data technologies such as 'Hadoop' and cloud-based analytics bring significant cost advantages when it comes to storing large amounts of data and enable businesses to identify more efficient ways of doing business.
2. **Faster and better decision making**. With the speed of Hadoop and in-memory analytics, combined with the ability to analyse new sources of data, businesses are able to analyse information immediately – and make more accurate decisions, devoid of human error and discrimination, based on what they've learned.
3. **New products and services.** With the ability to gauge customer needs and satisfaction through analytics comes the power to give customers what they want. With Big Data analytics, more companies are creating new products to meet customers' needs.

Increasingly businesses incorporate the ability to communicate continuous feedback about how their product is performing in the product itself. This machine data not only drives innovation and value, but also the exponential growth of data and the need for greater data infrastructure to manage this.

Sources

4. Computer Weekly, "Holographic data storage: the next big thing?", 2007
5. International Institute for Analytics, "Big Data in Big Companies", 2013

Ultimately, however, it is personal data on the customers behaviour and experience of the product that matter most to businesses and where the biggest advances in AI are possible. To be clear, businesses don't want to know about the individual per se. For machine-learning processes to learn best, they need to know what the person, and people do en masse.

This means that for businesses, being able to aggregate big amounts of anonymous and de-identified (see Glossary) personal data is everything. Big Data aggregation is key to business. Whilst retaining identifiable personal details can be useful for creating integrated datasets used to carry out enormous social impact particularly by charities, NGOs, and governments in delivering silo-breaking approaches to delivering public services, this is not the same as AI and machine learning.

To this end, data protection regulation is there to ensure that identity, security, and consent are not compromised in the process of collecting, storing, transferring, and processing personal data into the Big Data useful for business. Not only this, but without appropriate checks and balances, algorithms used in machine learning can be at risk of replicating the inherent biases and discrimination that exist in the individuals from whom data is collected. This makes appropriate protection and safeguards for the collection, storage, transfer, and processing of personal data a priority for both businesses and governments.

2.4 THE VALUE OF DATA TO TECH-TRADE

Tech-trade, defined by UKIBC, is the free trade and transfer of technological and digital products and services (including data) between individuals, businesses, and countries.

Despite growing exponentially, rapid advances in collecting and storing data mean that transferring and trading data-sets, metadata, and Big Data across borders is easier than ever before. This enables businesses to collaborate and match the comparative advantages in AI research in one country with the caches of data it needs to function from another country. This achieves far more together than each country's businesses can achieve alone.

Indeed, in its report 'No Transfer, No Production', the Swedish Board of Trade describes how the 21st Century can in many ways be summarised in two concepts[6]:

1. The fragmentation of production into geographically dispersed Global Value Chains (GVC).
2. The digitisation of production and trade including the subsequent need to move digital information or data.

Digital innovation is rapidly defining 21st century international trade with clear opportunities for those with a competitive advantage in AI and data. The

Sources

6. Kommerskollegium, "No Transfer; No Production", 2015

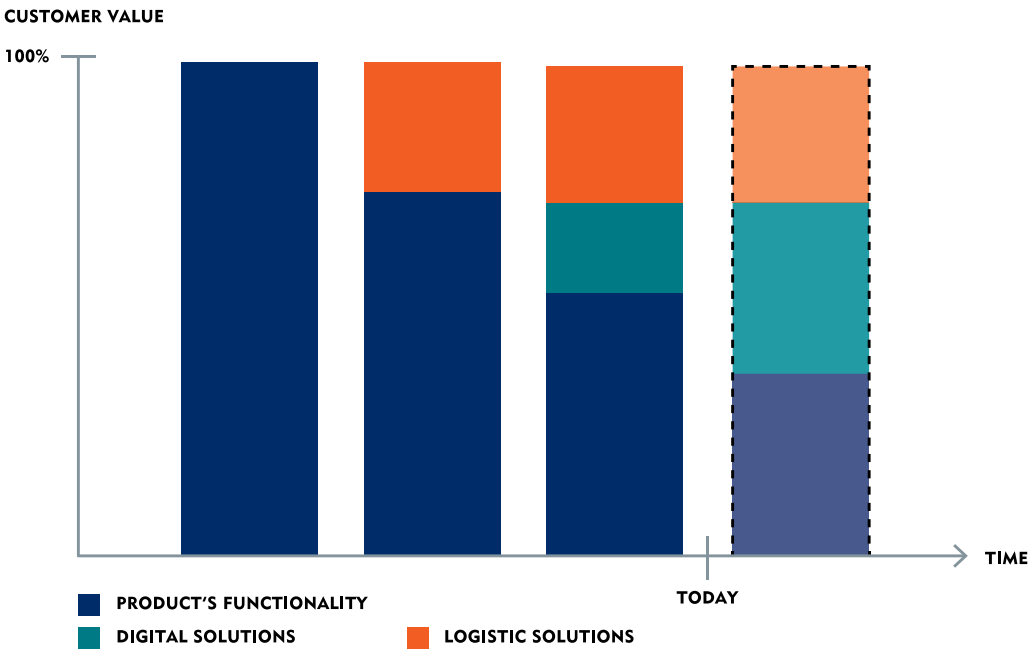
digital economy already accounts for 25% of global GDP, with the value of cross-border flows surpassing the value of merchandise trade for the first time in 2015. Half of all value created in the global economy over the next decade will be digital. In short, tech-trade, is rapidly becoming the third pillar of international trade alongside goods and services.[7]

Access to cross-border transfers of data is therefore vital to international trade, investment, and collaboration. Just as data is evolving, global trade is also evolving as traditional and outdated patterns of dominant north-to-south global trade give way to increasing trade between emerging south-to-south nations. This means the rules and regulations governing emerging tech-trade cannot follow the same patterns of the past in goods and services.

Embracing this is about both businesses and nations staying competitive and driving value for consumers. However, even customer 'value' is far from a fixed concept. For instance, in manufactured goods customer value used to be based solely on the functionality of products and subsequent productivity increases. Over time though, customer value has now moved toward being a package of solutions that benefit the customer starting with an efficient logistics solutions as a way to increase value. Today more and more value is found in digital solutions, IoT solutions, and further on intelligent machinery. As consumer value changes, adoption of data must be able to move with demand. What is clear however, is that barriers to cross-border data transfers means less value for customers and less competitive production.

GRAPH 3 - CHANGE IN PRODUCT VALUE OVER TIME

ILLUSTRATIONS OF CHANGES OVER TIME IN WHAT CREATES VALUE FOR CUSTOMERS



Based on work by the Swedish National Board of Trade

Sources

7. Information Technology and Innovation Foundation, "The Digitalization of Modern Manufacturing", 2017

Savvy regulators must bear this in mind when regulating cross-border data transfer. This is not the same as saying that data transfers should not be regulated or that a high level of data protection is automatically a barrier to trade. On the contrary, strong protection of data can entail a competitive advantage by increasing trust, and it is not uncommon that firms take advantage of restrictive data regulation to develop competitive advantage and better their business offers.

Therefore, when regulators seek to strike the right balance between minimising the misuse of data and maximising its immense potential, they must increasingly ensure that companies and customers alike are able to reap the benefits that cross border data movement offers.

3. TAKING THE UK-INDIA TECH PARTNERSHIP TO ITS FULL POTENTIAL

UK India Business Council firmly believes that there is a mutual and unique advantage to both India and the UK in digital bilateral cooperation and collaboration.

At the same time, for UK-India collaboration to truly flourish, it is crucial for both Governments to recognise the importance of tech-trade in data, technology, and digital innovation in our future bilateral relationship. Whilst both Governments play an enabling role in encouraging more horizontal grassroot business connections between both countries, the onus is also on UK and Indian companies to unite and deliver our immense collaboration potential.

This section brings to light the complementary ambition, expertise, and resource the UK and India each bring to the table as future leaders in AI and data, particularly in the healthcare sector. Through this we show how an ambitious UK-India Tech Partnership could unlock our unrivalled and stark complementarities for collaboration in the form of a 'UK-India Common Data Agreement' (CDA).

The UKIBC defines a UK-India CDA as a government-to-government agreement enabling the pooling of both UK and Indian de-identified, an anonymous, personal data for equal access by businesses and organisations from both countries. Under such a framework, UK and Indian businesses can combine their expertise using sandbox and open source protocols to innovate and develop key technologies aligned to the objectives of both Governments.

Crucial to this is acknowledging the adequate levels of data protection provisions and safeguards in each other's jurisdictions.

In drafting its Personal Data Protection Bill, there is, therefore, massive opportunity here for India to propose forward-looking regulation balancing the needs of individuals, businesses, and international trade in truly maximising its AI ambitions.

3.1 THE UK: A PIONEER IN DATA AND AI

The UK tops the 2018 global Government AI Readiness Index and is a world leader in exporting innovation and technology.[8] With a comparative advantage in providing a platform for AI innovation and dissemination, as well as being a leader in developing ethical standards for AI adoption and cybersecurity, there are compelling complementarities between UK AI expertise and India's data opportunity.

Sources

8. Oxford Insights, "Government AI Readiness Index", 2018

The UK Government actively aims to be a positive and enabling influence for the uptake of AI in existing businesses, as well as the creation and rapid up-scaling of new AI and tech-based startups. Indeed, building on the UK's global head-start in AI expertise, the Government has ensured AI is a core component of the new UK Industrial Strategy.[9]

The subsequent publication of the 'AI Sector Deal' (due to be reviewed in early 2019) outlines a national AI strategy focussed on the five foundations of the UK Industrial Strategy:[10]

- **Ideas -** Support AI innovation to raise productivity
- **People -** Attract the best talent globally, and invest in developing a bigger and more diverse AI workforce with widespread data-literacy across all sectors
- **Infrastructure -** Enhance the UK's existing data infrastructure including developing fair, equitable, and secure data sharing frameworks that deliver a strong digital and telecommunications infrastructure across the UK
- **The business environment -** Ensure global AI leaders look to headquarter in the UK. Support high growth and the rapid up-scaling of AI businesses complimented by an AI global export strategy
- **Places -** Invest in the development of tech-cluster cities across the UK including 'Tech-City UK'

The aim is clear: rapidly grow the UK's AI capabilities and expertise by attracting global talent to the UK, and developing home-grown, high-quality businesses, people, and innovation here that are connected and exported the world-over. This is a bold and proactive strategy that reflects ambitions for AI to account for £200 billion, or 10%, of UK GDP by 2030.[11]

Though UK success has been primarily driven by business innovation, the UK's leadership in the ethical application of AI very much stems from the early adoption of an active, well resourced, tech-savvy data protection authority. The UK's Information Commissioner's Office (ICO) came into existence 35 years ago, and has now firmly established itself as the largest data protection authority in the world working actively alongside businesses, innovators, and international authorities to deliver the best in regulation.

3.2 INDIA: AN IMMENSE AI OPPORTUNITY

The size of India's future data cache brings a new meaning to the term 'Big Data'. Amounting to 40,000 petabytes in 2010, digital data in India is likely to grow to 2.3 million petabytes by 2020 – twice as fast as the global rate of growth.[12] If India houses all this data, it will become the second largest investor in the data centre market, and the fifth largest data centre market globally by 2050.

Roll out of the Aadhaar biometric identity card scheme has reached 1.1 billion citizens, whilst drives to digitalise government interactions have seen

Sources

9. Department for Business, Energy, and Industrial Strategy, "The UK's Industrial Strategy", 2018
10. Department for Business, Energy, and Industrial Strategy, "AI Sector Deal", 2018
11. PWC, "The economic impact of artificial intelligence on the UK economy", 2017
12. Cushman and Wakefield, "India Poised for Massive Data Center Growth", 2018

93% of all India taxes being paid online, resulting in an impressive 80% jump in tax returns filed in the last 12 months.[13] Meanwhile the Government is developing plans that will see the largest health insurance scheme in the world [Ayushman Bharat] set to be totally digital. This, coupled with exponential growth in the use of social media and e-commerce platforms, sets India on a course to arguably become the most data-rich country in the world.

In this context, some studies have shown that if AI is adopted to its full potential, India's AI stands to be worth $3.14 trillion, equivalent to 20% of the global AI market, by 2030.[14] India ranks third in terms of penetration of AI skills among their workforce.[15] With advancements in machine learning and deep-learning algorithms, AI is expected to thrive if allowed access to the mines of Big Data being collected in India.

India has already seen explosive growth in the number of Internet users, fuelled by the private sector's efforts to tap vast new markets and government investment in modernising the country's tech infrastructure. According to statistics published by the Telecom Regulatory Authority of India, India consumed almost 22% of the world's mobile data between April and June 2018.[16] India's Internet penetration and technology absorption rate is one of the fastest in the world, which is generating huge demand for digital services across all sectors and provides great scope for UK-India collaboration.

India's AI potential is clearly phenomenal. This is only growing and the Indian Government has been right to recognise this. In 2015, the Government launched 'Digital India' which has been crucial in enabling the mass roll out of Aadhaar Biometric identity cards, the Bharat Broadband Network (BBNL), and the Centre of Excellence for the Internet of Things (COE-IT). This programme has been pivotal in generating the cache and infrastructure that exists today and kick started an AI-ecosystem.

This is only gathering pace. In the 'Interim Budget' delivered by interim Finance Minister Shri Piyush Goyal in February 2019, the Government proposed the launch of a National Programme on Artificial Intelligence to be kick-started by the creation of a 'National Centre on Artificial Intelligence' and a 'National Artificial Intelligence Portal' as overarching hubs bringing together a developing network of Centres of Excellence.[17]

An unwavering commitment to establish and grow India's data cache, infrastructure, and expertise is the right approach as a springboard for business collaboration to unleash India's AI potential. Both UK and Indian Governments have acted as enablers. In India, the Government's efforts have thus far been clear and focussed towards[18]:

- Enhancing the potential economic impact of AI for India.
- Harnessing AI techniques for social development and inclusive growth tackling the big, global socio-economic problems that exist in India.
- Building an 'AI Garage' of data and expertise making India the go-to solution provider for emerging and developing countries representing 40% of the world.[19]

Sources

13. Economic Times, "Two crore Indians file returns but pay zero income tax", 2018
14. The Hindu Business Online, "AI, a $3-t opportunity for India", 2018
15. LinkedIn, "The Age of AI is Here. Here's How to Thrive In It", 2018
16. CNN Business, "The Future of the Internet is Indian", 2018
17. UKIBC, "Highlights from India's 'Interim Budget' 2019", 2019
18. London Business School review Issue 3, "How AI is advancing across the world map", 2018

This strategy focuses on maximising India's 'latecomers advantage' to reboot the national business process outsourcing (BPO) sector through advanced IT and ITS sectors. Essentially, this represents a 'solved in India by Indian companies' model for companies to carry out their technological development in India.

The UK is already a close partner of India's BPO sector and the UK and India should build on these foundations to build an "unbeatable combination" in AI and the broader digital space. Looking to operate in different markets, but with a similar approach to the advancement of AI platforms, upstream AI business development, and a mutual approach to AI's ethical applications the UK and India are clear companions, not competitors. Together, we have enormous complementaries between our respective global comparative advantages in order to help each other's businesses to achieve far more than could be done alone.

3.3 INDIA'S FIVE PRIORITY SECTORS FOR AI:

NITI Aayog's recent report on the potential of AI in India makes the case for formalising AI governance to meet these ambitions, and deserves careful examination from the perspective of how UK-India business collaboration can deliver on these priorities.

Through further advancing research avenues, skill development, and creating an apt data marketplace with incubation hubs to encourage better implementation, NITI Aayog highlights five strategic sectors formal AI policy could transform:

TABLE 2 - NITI AAYOG'S FIVE PRIORITY SECTORS

NITI AAYOG SECTOR	KEY TARGETS
HEALTHCARE	Well-being. Early detection. Diagnostics. Research and training
AGRICULTURE	Soil health monitoring and restoration. Increasing the efficiency of farms. Increase in the share of price realisation to producers.
EDUCATION	Adaptive learning tools for customised learning, intelligent and interactive tutoring systems. Predictive tools to inform pre-emptive action for students predicted to drop out of school. Automated rationalisation of teachers. Customised professional development courses.
SMART CITIES AND INFRASTRUCTURE	Smart parks and public facilities. Smart homes. AI driven service delivery. Crowd management. Intelligent safety systems.
TRANSPORTATION	Autonomous trucking. Intelligent transporation systems. Travel route/flow optimisation. AI for railways. Community based parking.

Sources

19. NITI Aayog, "National Strategy for Artificial Intelligence, 2018

The right approach to regulation and international collaboration can deliver on India's AI priorities.

To illustrate this potential in more depth, we investigate how UK-India data and AI collaboration could transform India's healthcare sector - a top priority for the Government and its citizens.

3.3.1 How AI can deliver India's healthcare ambitions

"A lot of the challenges to healthcare in India can be resolved with AI" - NITI Aayog Adviser, Ms. Anna Roy[20].

The adoption of AI in Indian healthcare can significantly improve the efficiency, quality, cost, and reach of healthcare. This could not come at a more valuable time, as the introduction of the 'Ayushman Bharat' scheme promises to expand health insurance to all Indians.

However, India already requires 7.4 million healthcare professionals by 2022, more than double the existing workforce, whilst Ayushman Bharat recipients will rightfully expect more and higher quality healthcare as access to more complex procedures grows.[21]

There is a clear and significant gap in the skills, resources, and reach to delivering India's healthcare ambitions that AI can directly bridge in three tangible ways through the use of[22]:

Descriptive AI - Most commonly used today, descriptive AI is useful for monitoring trends in a patient's condition that are otherwise hard to detect. It enhances decision-making taken by existing practitioners by providing them with more accurate and frequent information.

Predictive AI - Uses descriptive data to make predictions about a patient's condition, identify conditions early, and help hospital management by prioritising patients, providing real-time reports, and planning admissions. In short, it augments decisions taken by practitioners.

Prescriptive AI - Furthers the purpose of predictive AI by detecting trends that may not be predicted by humans, and suggesting treatments. Here, prescriptive AI can replace the need for a human decision maker whilst being subject to review by practitioners.

Sources

20. Anna Roy, NITI Aayog Adviser, speaking at the India-UK Futuretech Festival's "Innovation: The Future of Healthcare" session, 2018
21. National Skill Development Corporation, "Human Resource and Skill Requirements in the Healthcare", 2015
22. The Center for Internet and Society, "Artificial Intelligence in the Healthcare Industry in India", 2018

Niramai

CASE STUDY

NIRAMAI - NON-INVASIVE, PORTABLE,
PRIVACY-AWARE BREAST CANCER SCREENING SOLUTION

Occurring in 25.8 people for every 100,000 women and with a low survival rate of 66% as compared to 90% in the US or Australia, breast cancer is the primary cause of cancer-related deaths amongst the Indian female population. One of the main reasons for such a low survival rate is late detection of the cancer. Here, Mammography is considered the gold-standard in screening.

However, it is invasive and relatively expensive due to the capital cost of equipment and the need for experienced radiographers. Mammography is though effective in early detection as other methods of screening are only effective after the tumor has grown.

Niramai has found another way. They have created and trained proprietary machine learning models to identify tumors from high resolution thermal images. With supervised clinical trials on over 4000 patients, their method has shown over 90% sensitivity, 27% higher accuracy than Mammography, more reliable predictions, and an ability to detect cancer lesions as small as 4mm with no palpable lumps.

This alternative screening method poses zero-radiation exposure, higher accuracy, low capital cost of equipment, and the ability to screen younger age groups - overcoming several limitations to Mammography and other methods. By being low-cost, non-invasive, privacy-aware and painless, it increases the accessibility and affordability of breast cancer screening.

3.3.2 Challenges in meeting India's AI healthcare potential

"The obstacle to AI implementation in healthcare is not technological but access to data. Research is hampered by difficulties in accessing large medical datasets, for legal or other reasons. It's particularly tough for startups in the field; larger players already have access to such data."[23]

However, several challenges remain to applying AI where it is most needed in India. The main challenges for healthcare providers using data in India relate to consent for collection, ensuring that the data is clean and uniform, and transfer across borders.

In 2016, the Electronic Health Records Standards (EHR) introduced attempts to address some of these concerns by regulating ownership and privacy of patient data when stored and transferred. This includes data collected through medical establishments, medical devices, and self-care systems. It's data ownership and access provisions require strict patient consent, though data can be freely transferred and processed within India without the need for permission so long as it has been de-identified.[24]

Sources

23. The Economist Intelligence Unit, "Artificial Intelligence in the Real World", 2016
24. The Wire, "Without Data Security and Privacy Laws, Medical Records in India Are Highly Vulnerable", 2017

Though this appears positive in principle, implementation of the EHR has been hounded by different interpretations of how records should be digitalised, retained, and accessed both within and between hospitals. The EHR also lacks a standardised approach to anonymisation. Although this allows for greater flexibility amongst companies adopting self-regulatory practices of anonymising data before using it further, it also places barriers to using data in international research and collaboration.

Legal barriers in the form of data residency and security relating to the flow of data prevent organisations outside India from accessing healthcare data. This is a problem also faced by EU countries under the GDPR which lays down strict parameters regarding data transfer that can act as a barrier to life-saving innovation.

A current draft bill entitled the 'Healthcare Data Privacy and Security Act' aims to tighten penalties to data breaches whilst outlining clear principles for data collection, use, and transfer between private hospitals. However, taking a sector-level approach to data protection regulation runs the risk of overlapping jurisdictions and confusion as to how different provisions interact.

The slow development of regulation supporting and enabling healthcare data and AI development is matched by the lack of infrastructure on the ground to meet healthcare demand. One of the major barriers to delivering any form of healthcare to many Indian's is geography. Last mile delivery of healthcare services is a major challenge, as 69% of the population reside in rural areas.[25]

Rural populations could gain access to diagnostic facilities and treatment knowledge through preventive and predictive technologies. Predictive modelling of diagnosis data and patient health records will help to identify and prevent disease outbreak. However, this relies on villages having reliable and cheap access to electricity, devices, and internet connectivity. Even non-electronic data, such as hospital records, are unreliable and difficult to convert into an accessible, uniform digital format.

The inconsistent application of the EHR combined with a lack of secure infrastructure, has also exposed both hospitals and businesses to criminal activity exploiting cyber-security loopholes. This makes keeping healthcare records safe a daily challenge which needs to be tackled as a first step in delivering India's healthcare ambitions.

3.3.3 The opportunity for enhanced UK-India healthcare collaboration

Both UK and Indian Governments highlight healthcare as a sector where the full application of AI could be transformative on a socio-economic scale like no other.

In India, the Government has pressed ahead with several initiatives to support the adoption of AI across five key areas in hospitals: pharmaceuticals,

Sources

25. The Business Standard, "670 million Indians in rural areas live on Rs 33 per day", 2015

diagnostics, medical equipment and supplies, medical insurance, and telemedicine. These initiatives include the National e-Health Authority, Cognitive Science Research Initiative, Biotechnology Ignition Grant Scheme, and the Centre of Excellence for Data Science and Artificial Intelligence.[26]

In the UK, the Government has equally acted as an enabler, announcing a £50 million investment towards launching five new medical technology centres in Leeds, Oxford, Coventry, Glasgow, and London in 2019.[27] These centres will be using AI in early detection, pattern recognition, patient scans, diagnosis, research, and training.

The UK Government has further pioneered collaboration with business in delivering the new 'GP at Hand' service currently being trialed in the London area where residents can book and carry out consultations with GP's through the Babylon app.

The UK holds a leading role in the application and innovation of AI in healthcare whilst India is just setting out. The key to unlocking India's AI potential will come through systemic regulation that allows businesses to bring together India's immense data wealth and UK expertise, innovation, and resource.

Already, the immense opportunity UK India AI collaboration could offer healthcare is being recognised with the launch of a Healthcare AI catalyst at the 2018 India-UK FutureTech Festival in Delhi.[28] The catalyst represents an important step for collaboration between the UK's Department for International Trade and the Indian Government think tank, NITI Aayog. With £1 million in funding, the programme will enable some of the best AI healthcare companies from the UK to deploy solutions to problems faced by Indian public hospitals.

Whilst such first steps are promising, they are modest. The full UK-India AI healthcare potential can only truly be unlocked through clear, standardised, and enforced regulation protecting patients whilst allowing business-led collaborative innovation. Regulation that achieves this would pave the way to an enhanced agreement between the UK and India that recognises each others' adequate data protection standards, and would allow for the transfer of each others data securely.

As former Chair of NHS England. Sir Malcolm Gladwell, said at the India-UK FutureTech Festival in 2018, "Regulation, privacy, and access to data will propel AI in healthcare".[29]

Sources

26. The Center for Internet and Society, "Artificial Intelligence in the Healthcare Industry in India", 2018
27. Verdict, "UK government announces £50m funding for AI in healthcare", 2018
28. UKIBC, "The Tech Collaboration Defining India's Healthcare Horizon", 2018
29. Sir Malcolm Gladwell, Former Chair of NHS England, speaking at the India-UK FutureTech Festival session "Innovation: The Future of Healthcare", 2018

CASE STUDY

BUGWORKS - DRUG DISCOVERY AIDED AND ACCELERATED BY AI

Drug-resistant infections kill around 700,000 people worldwide each year, and this figure could increase to ten million by 2050. In India alone, superbugs kill nearly 60,000 newborns every year.

Drug discovery is a long and complex process with multiple failure points. To test and develop effective new assets against superbugs, the Bugworks team has been using AI. Bugworks have created a computational platform where the network is built to copy the behaviour of the microbe in an infection. The company found a supportive ecosystem of hospital partners who share data on an ongoing basis which keeps their simulation network updated.

With continuous stream of real-world data, richly annotated scientific information, and a simulation network with AI, the Bugworks team has built a unique set of tools to aid the process of drug discovery. This resulted in a significant in-laboratory testing time. The company hopes to convert some of these assets into lead compounds that will enter human clinical trials in a couple of years. A new drug that used to take 12 to 15 years under development, could now take only 5 to 7 years, and end up saving millions of lives globally.

3.4 RE-THINKING THE FUTURE OF THE UK-INDIA TECH PARTNERSHIP

This report has laid out the central role data and AI will play in enabling business and trade in the not too distant future. The clear complementarities that exist between the UK and India here make possible unprecedented collaboration to deliver this immense opportunity.

The UK-India Tech Partnership was launched by Prime Ministers May and Modi in April 2018 to identify and pair businesses, venture capital, universities, and entrepreneurs towards enhancing innovation and adoption of technology.[30]

This partnership builds on an already strong trade and investment relationship. In 2017, India's stock of FDI in the UK was £8 billion, a huge 321% increase on 2016, representing the largest growth of any country in the UK in the last decade. In turn, the UK is the largest G20 investor in India.[31]

Of Indian investments in the UK, 31% are in tech, accounting for 33,000 of the 110,000 jobs created by Indian companies in the UK.[32] The UK exported £344 million of digital services to India in 2016, and is India's second largest bilateral science partner.[33] Indeed, under the Newton-Bhabha Partnership, India-UK collaborations will have risen from £1 million in 2008 to over £400 million by 2021.[34]

Sources

30. GOV.UK, "UK and India agree ambitious new tech partnership", 2018
31. UK Department for International Trade, "Overseas investment into the UK at highest ever level", 2018
32. Grant Thornton, "India meets Britain Tracker", 2017
33. British High Commission, New Delhi, "UK-India celebrate Tech Partnership at FutureTech Fest", 2018
34. British Council, "Newton Bhabha Fund"

The foundations for launching the UK-India Tech Partnership are therefore self evident. UK and Indian businesses want to do more business with each other, and technology will be crucial to underpinning this.

Since its inception, the Tech Partnership has already delivered notable achievements including the announcement of the first two Tech Cluster Partnerships in the form of the Midlands Engine-Maharashtra partnership to explore future mobility, and the Northern Powerhouse-Karnataka partnership focusing on AI and data.

This was followed up by the first India-UK FutureTech Festival in Delhi in late 2018, bringing together leading decision makers, businesses, think-tanks, academics, and experts under the same roof with the same purpose: to explore UK-India tech collaboration. It was at the FutureTech Festival that the £1 million Health Catalyst was launched to bring UK AI healthcare expertise to bare on the problems faced by India's public hospitals, and during which the first meeting of the UK-India Future Manufacturing Steering Group took place.

Government-to-government exchange has followed a wealth of industry collaboration. Tech solutions firm Equiniti Group opened a new digital lab in Bengaluru in January 2019, creating hundreds of new jobs.[35] UK telecoms company BT is partnering with one of India's leading research institutes, the Indian Institute of Science (IISC), to launch a new collaborative research centre, also in Bengaluru.[36] Venture capital firm Pontaq has launched a £50 million fund designed to create over 2500 jobs in fintech, smart cities tech, and emerging tech across the UK and India.[37] The list goes on.

Whilst both Government's have played a commendable enabling role in supporting a business-driven tech partnership, the most significant regulatory barriers to achieving our AI potential still remain, and so far neither Government's commitment to the partnership has sought to address them. These barriers are the adequate protection and free transfer of Big Data which form the lifeblood of AI, machine learning, and innovation.

Businesses are supportive of the Partnership and they are also impatient for further progress. A business scope of the Partnership is under preparation but it will be some months before it is signed off within the UK Government.

It is timely that, on the back of NITI Aayog's publication last year of a National Data Strategy, India seeks to introduce its own Data Protection Bill, minimising misuse and maximising trust and innovation. Against this background, now is also the right time for both Governments to step up the UK-India Tech Partnership through greater engagement with UK and Indian businesses on Data Protection Regulation, Tech-trade, and AI Innovation.

Sources

35. Equiniti, "Equiniti's New Bengaluru Digital Hub Lauded By Senior Officials As "Superb Investment Project" For India's Tech Capital", 2019
36. UKIBC, "BT and Indian Institute of Science to establish a collaborative research centre in Bangalore", 2018
37. British High Commission, New Delhi, "UK-India celebrate Tech Partnership at FutureTech Fest", 2018

A UK-INDIA JOINT DATA GARAGE

This is why the UKIBC would encourage both Governments to create a joint virtual "Data Garage" enabling businesses of both countries to pool and transfer de-identified and anonymous personal data freely so as to produce technical solutions, initially in the area of healthcare. Such a mechanism could be monitored via a government-to-government UK-India Common Data Agreement (CDA) opening up one of the major areas on business-to-business collaboration delivering new technologies in areas of mutual focus for both the UK and India.

Using "Sandbox" protocols, such a business-led "Data Garage" could be designed to encourage sharing and innovation, particularly in healthcare. Underlying this should be freedom of access and movement of metadata and datasets to foster that technological innovation environment. Such a mechanism, would allow for controlled open-source innovation and would also allow both Governments initiatives, in terms of the "National Centre on Artificial Intelligence" and the UK's newly announced five new medical technology centres, to link in to the 'sandbox' thereby creating a powerful multifaceted initiative.

Whilst taking this first step in healthcare has evident advantages, the scaleable potential this mechanism could deliver across NITI Aayog's five priority sectors for AI deserves just as much recognition.

This would represent a bold and pioneering commitment by both Governments to making the most of our unique complementary capabilities in AI and data. In

the wake of Brexit, all eyes will be on forging new collaborations with emerging global markets, however these have traditionally been negotiated for goods and services with minor acknowledgement of the value tech-trade offers in and off itself.

International treaties have been previously been negotiated between the UK and France, allowing for the sharing of sensitive defence and security information and data. This shows that it is possible and desirable to achieve a CDA that is sensitive to the provisions and safeguards that must be in place to protect sensitive data such as health records.

Given the unique and 'unbeatable' complementarities between the UK's expertise, finance, and innovation, and India's data wealth and ambition, no single step could improve the ease of doing business environment further than a bilateral agreement on the free transfer of data.

Crucial to forming a CDA is a mutual acknowledgement that each authority has adequate regulations and safeguards in place to ensure trust and security in international data access and processing. However, in evaluating India's draft Personal Data Protection Bill, we believe that the outline of a positive framework is in place subject to adequate clarification, checks, and balances.

4. INDIA'S PERSONAL DATA PROTECTION BILL 2018 AT A GLANCE

Data protection in India is currently based on the Information Technology Act, 2000 (IT Act) which is complex, sector specific, and lacks a holistic overview of the challenges of holding the largest data cache in the world.

The failings of the IT Act were exposed by Justice K.S. Puttaswamy in the case '*Retd. v. Union of India*' which led to privacy being recognised as a fundamental right. Duty bound to enact robust legal mechanisms to empower citizens against the infringement of their data privacy, the State responded with the draft Personal Data Protection Bill.[38]

The draft Bill, appears to be striking an approach grounded in the principles of qualified consent and qualified access.

The objective of the bill is to ensure a free and fair digital economy and is a critical step in setting up a privacy framework which gives the Indians the ability to effectively protect their personal data whilst promoting business and innovation in AI.

Whilst initial consent is required by the data fiduciary (the organisation using and processing the data) from the principal (the person whose data is being used), once given there is qualified recourse for the principal to retract consent.

This approach could hold enormous advantages for businesses collecting, processing, transferring, and using data, however questions remain as to the power this grants the Executive and the independence of the Data Protection Authority.

In this chapter, we briefly outline the eleven key provisions of the draft Data Protection Bill 2018, and contrast these with the dominant Data Protection approaches that exist globally in order to evaluate what this might mean for UK businesses, collaboration, and trade.

THE BILL TO DATE

JULY 2017

the Ministry of Electronics & Information Technology (MEITY) set up the Justice BN Srikrishna Committee to draft a data protection law.

NOVEMBER 2017

the Committee releases a White Paper outlining seven key principles of data protection for public comment.

JANUARY 2018

Four rounds of public consultations held inviting stakeholders to give their suggestions on the draft data protection framework.

JULY 2018

MEITY releases Justice BN Srikrishna Committee Experts' report on Data Protection and the first draft of the Personal Data Protection Bill, 2018.

Sources

38. Committee of Experts under the Chairmanship of Justice B.N.Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", 2018

4.1 KEY PROVISIONS OF THE DRAFT PERSONAL DATA PROTECTION BILL, 2018

1. Jurisdiction
Both the draft Bill and the GDPR apply exclusively to personal data. The Bill applies to the processing of personal data in India and the processing of personal data by firms incorporated in India. It also includes an extra territorial clause expanding jurisdiction to non-Indian incorporated firms processing data originating from their business operations in India.

The report, 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', accompanying the draft Bill suggested that jurisdiction should not include data of people not-present in India in order to avoid a conflict of different personal data protection laws across jurisdictions, particularly in the business process outsourcing (BPO) industry.

2. Lawfulness of Processing
Personal data may only be processed lawfully with the explicit initial consent of the principal. Like the GDPR, the draft Bill does however specify exemptions from explicit consent including:

- Functions of the Legislature bodies or State
- Compliance with law or order of a court
- Prompt action to protect vital interests
- 'Employment' purposes
- 'Reasonable' purposes

Where the GDPR explicitly allows for processing in cases where the data principal is party to a contract, under the draft Bill this is subsumed under the meaning of 'consent' to mitigate complications from separate contract clauses.

'Reasonable purposes' applies to data processing necessary for identifying and preventing unlawful activities such as fraud, network and information security. However, this list is non-exhaustive and contains little precise detail, opening it up to the risk of misuse by making it easier to bypass consent. The clause may also be used to justify processing in the data analytics industry, for the sake of beneficial technological innovations.

3. Right to Confirmation and Access
The right to confirmation ensures the principal has a right to know if and how their data is being processed by the fiduciary. This is similar to the right to access which ensures that the principal can access their personal data whether processed or not.

Though both the GDPR and the draft Bill provide strict provisions to safeguard the interests of the data principal and their ability to hold the data fiduciary accountable, the draft Bill differs significantly in the level of access it affords. Instead, it favours more restrictive access in which the principle is simply

allowed to request a brief 'summary' of their data being processed.
The inability of the data principal to obtain their personal data being processed also prevents them from properly exercising other rights, including the ability to rectify erroneous data if they are not aware of its usage by the fiduciary.

4. Right to be Forgotten
Both GDPR and the draft Bill have made this right available to the data principal but differ in both definition and enforcement. Under both, the right to be forgotten is not absolute, but subject to qualifications.

The draft Bill only allows the data principal to restrict disclosure of their personal information, subject to the approval of an adjudicating officer once an application form has been submitted. However, it cannot be erased from the data fiduciary's records, as is possible under GDPR.

The Bill's comparatively restrictive provision is based on the principle that erasure of publicly available information restricts other people's right to information and infringes on the right to freedom of expression and speech. Hence, any request for the right to be forgotten must clear the balancing test between the right of free speech and right to information.

5. Automated Processing
While GDPR gives the data principal the right to be informed of, object to, and opt out of automated data processing, the draft Bill offers none of these as this would enable ad-hoc human intervention to influence, prejudice, and bias automated decision-making by inserting an unnecessary step of human review.

Instead the Committee, in their report, take the approach that bias in automated processing should be addressed through an accountability framework. This would require data fiduciaries making evaluative decisions through automated means, to set up processes that preempt prejudice and 'weed out' discrimination.

This would be overseen by the DPA and where un-intended, albeit lawful, discrimination still occurs in processing, principles can approach the courts to remedy this.

"The interests underlying such rights can be more efficaciously achieved by an ex ante accountability model"[39]

6. Data Breach Notifications
Under GDPR, both the Data Protection Authority (DPA) and the principal need to be notified of any serious data breach affecting the principal's rights and freedoms. The draft Bill, however, only requires the data fiduciary to notify the DPA. The DPA then decides whether the data principal needs to be notified.

This is intended to avoid negative publicity and fear of liability that dis-

Sources

39. Committee of Experts under the Chairmanship of Justice B.N.Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", 2018, P.g.75.

incentivises fiduciaries from reporting breaches. The DPA therefore acts as an intermediary in informing the data principal, suggesting remedial measures, and deciding on the severity of the breach that needs to be reported based on whether it poses them harm that would require preventative steps to be taken.

The provision is concerned about the limited legal and technical understanding amongst most citizens which allows for undue alarm to spread if breaches are not handled appropriately. In the event of a data-breach, the DPA is treated as better placed to issue clarification and assurances than the fiduciary or principal.

7. Data Transfer

Both the GDPR and the draft Bill closely matches in allowing for data transfer to other countries on the following basis :

- **Adequacy Decision:** If another country, sector within a country, or international organisation provides adequate personal data protection provisions.
- **Appropriate Safeguards:** If the data transfer is being done with robust and sufficient safeguards in place.
- **Exceptions:** if there are certain exceptions granted to that particular transfer under GDPR or by the Indian DPA for their respective jurisdictions.

8. Data Localisation

The GDPR allows EU member states to decide themselves on the extent of localisation and transfer restrictions to certain countries or organisations. Several members have adopted localisation requirements for personal data, such as Germany, which requires telecommunications metadata to be stored locally for security and law enforcement purposes .

The draft Bill, on the other hand, explicitly requires all the data under its jurisdiction to have a serving copy in India. Furthermore, certain categories of data, which have been classified as critical data by the Indian Central Government, must be processed only in India. This has been justified to ensure :

- More effective law enforcement
- Avoiding vulnerabilities of data transfer via fibre-optic cable network
- Promoting Artificial Intelligence (AI) and digital infrastructure in India
- Preventing foreign surveillance.

9. Exemptions

Whilst data protection laws aim to strengthen the position of the principal with respect to the fiduciary, both the draft Bill and GDPR make exceptions. In the draft Bill these are:

- Processing for the security of the state
- Processing for prevention, detection, investigation, and prosecution of

criminal activity.
- Processing for the purpose of legal proceedings
- Processing for research, archiving or statistical purposes
- Processing for personal or domestic purposes
- Processing for journalistic purposes
- Manual processing by small entities

This differs from the GDPR in several ways. The wording for the exemption for research purposes in the draft Bill implies a blanket exemption for all kinds of research unlike the GDPR, which limits this to archiving in the public, scientific or historical research interests.

The language used for these provisions in the draft Bill leaves broad scope for interpretation and possible misuse. For instance, in allowing the processing of personal data for purely personal or domestic purposes, this exemption becomes void if this involves 'disclosure to the public'. It does not, however, elaborate on the phrase 'public', opening it up to confusion. The GDPR on the other hand clearly specifies what is meant by 'public' disclosure.

10. Data Protection Authority

Under GDPR, the structure and functions of the DPA are left to Member States to decide within parameters. The draft Bill on the other hand, outlines this is a far more detailed manner.

Though DPA's established under GDPR and the draft Bill share common investigative, corrective, and advisory powers, the Indian DPA has the additional task of specifying additional categories of sensitive data. This includes defining 'reasonable purposes', according to which data can be processed without explicit consent.[40]

Given such rule-making powers, its decision-making structure is intended to be independent and immune to external influences. However, with a DPA Board, consisting of a Chair and six full-time members, appointed by the Central Government based on Select Committee recommendations, this brings its independence into question. This Select Committee is comprised of the following three members with significant scope for Government influence:

- A Chief Justice or a Judge of the Supreme Court nominated to act as the Chair
- A Cabinet Secretary
- An Expert nominated by the Chair in consultation with the Cabinet Secretary

11. Penalties

The draft Bill defines penalties for infringements to certain provisions, which much like the GDPR, are of either between two to four percent of the fiduciary's total worldwide turnover from the preceding year, or a fixed amount of IND 50 or 150 million, depending on which is higher.

Sources

40. Personal Data Protection Bill, 2018, Article 60

Unlike the GDPR however, obtaining, transferring or selling personal data illegally that results in harm to the principal, can result in criminal proceedings including a jail term of up to five years. Re-identification and processing of de-identified data without the consent of the data fiduciary or the data processor can be similarly punished with a jail term of up to three years.

Including criminal penalties in the draft Bill is intended to deter wilful violations of the law, and imply that the cost incurred by violators is proportional to the harm caused by them.

4.2 PLACING INDIA'S BILL IN A GLOBAL CONTEXT

India is one of the few upcoming superpowers to have not yet adopted a comprehensive approach to personal data protection.

However, data is increasingly difficult to define and control according to geopolitical borders and businesses using data to deliver innovation needed to operate across borders to deliver the best in innovation. Differences in the data protection laws across jurisdictions can therefore act as significant barriers to doing business. So, how does India's draft Bill place globally?

Justice B.N. Srikrishna's Expert Committee report outlined three distinct global approaches to data protection for India to learn and navigate from[41]:

1. The laissez-faire approach of the US
2. The human rights approach of the EU
3. The national security focus of China

The US approach largely relies on the limited privacy protections found in the First, Fourth, Fifth and Fourteenth Constitutional Amendments that give citizens a right to privacy. This has been put into practice through myriad data legislation without overarching legislation and sectoral laws governing personal data in the private sector.

The EU has attempted to set a 'gold standard' in personal data protection through the General Data Protection Regime (GDPR). The GDPR is technology and sector agnostic, putting in place a comprehensive legal framework that regulates the processing of personal data centred on the rights and obligations of the parties concerned. The GDPR therefore represents an informed consent approach.

Whilst allowing for the intensive use of data within its borders, China strictly controls the cross-border data transfer grounded in national security-based interests. China's rules are currently more opaque due largely to the absence of a personal information law, which is currently being prepared, and the existence of a cybersecurity law as a stop-gap measure.

Sources

41. Committee of Experts under the Chairmanship of Justice B.N.Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", 2018

The benefits and drawbacks of each approach are clear. The US approach allows large scope for innovation but also the potential misuse of data. The Chinese approach enables intensive data usage to scale up its AI industry quickly, however prohibits collaboration and provides little personal security. The EU approach allows individuals so much control over the use of their personal data that this also represents a barrier to innovation and AI whilst generating 'consent fatigue' among a population lacking understanding as to what they are being asked to consent to.

Although the GDPR will need review in the not too distant future, once its implications become evident, its broadly positive initial reputation means there is domestic political benefit for the Indian Government to be seen to talk about adopting a GDPR type model.

The risk for India, if it chooses something tightly modelled on GDPR, is that it embeds the same kind of competitive disadvantage that the EU has imposed on itself and does not give opportunity to use its immense data cache to its full potential in growing the economy and delivering on its socio-economic ambitions.

Nor, if India took this path, would it give itself the opportunity to stand tall in the face of regional competition with China, whose strategy is to use data processing intensively through both public and private actors to underpin its geopolitical dominance and national security.

Finding the right approach, therefore, has significant impact in the adoption costs businesses face, the national comparative advantage that emerges in AI, and India's wider ability to influence data protection best-practice globally as a truly 21st century superpower.

5. WHAT DOES THE BILL MEAN FOR BUSINESS?

What India has proposed in its draft Bill is a qualified-consent, qualified-access approach with enormous potential to facilitate both trust and trade. However, further clarity is necessary before businesses can be confident with processing data in India.

In this section, we evaluate the impact the draft Bill's provisions will likely have on UK businesses' ability to innovate, collaboration, and operate in India's data market.

5.1 A BETTER WAY FOR BUSINESS TO ACCESS AND PROCESS PERSONAL DATA

From the perspective of businesses using personal data, the draft Bill's provisions on the rights to be forgotten, confirmation, access, data breaches, and automated processing are potentially a significant improvement over that in the GDPR.

Once initial consent has been secured to automatically process personal data, it is costly and inefficient to reverse this if the principal decides to withdraw consent or enact their right to be forgotten. Indeed, these are provisions businesses are still trying to work out how to enforce in Europe which are already having a tangible impact on the region's AI and data competitiveness.

This is particularly the case once data has been anonymised or de-identified in a metadata format, which makes finding the original source principal difficult. Ensuring that individuals have the right to a summary of the high-level use of their personal data only goes a long way to addressing these concerns and making India an easier place to process data.

On both a practical and ethical level, the Government is right to be concerned that ad hoc intervention, such as through individuals seeking to be 'forgotten', risks unnecessarily introducing human bias and error into complex algorithms needed to clean, process, and translate data into AI outcomes. Though there is the risk of AI algorithms replicating the systematic bias and discrimination personal data already contains, it is the right approach for the State to require businesses to address this ethical concern early on as a fundamental part of building the data processing structure.

Likewise, we agree that requiring the principal to be informed of all and any data breaches concerning them directly by the fiduciary has the risk of spreading fear and misplaced confusion. Informing them in the instance of direct harm being caused is a sensible balance between maximising opportunity and minimising misuse.

However, to facilitate trust that the public notification of breaches will not be manipulated for political gain, strong assurance and clear guidelines need to be put into place making the notification procedure by the DPA fully independent, transparent and accountable. This includes defining 'harm' to the principal without ambiguity.

These clarifications are important to businesses and citizens alike in maintaining trust in the regulatory structure.

5.2 WHAT ARE THE FACTS ON DATA LOCALISATION?

Perhaps the most poorly understood provision is that for 'Data Localisation'. This needs significant clarification in order to reassure businesses that Indian data, on the most-part, can transfer freely across borders. Data transfer is the lifeblood of innovation, collaboration, and trade, which, if compromised, would have significant ramifications for India's AI ambitions.

That said, much emotion has been visible in India surrounding the question of data localisation. The Indian Government is already inclined towards local data storage in several policies and proposed legislation. This position has been supported by the Reserve Bank of India and by certain Indian sector groups as well as prominent Indian companies such as Paytm and PhonePe. At the same time, foreign Internet and digital companies have been lobbying through industry bodies for a reconsideration of data localisation provisions.[42] Moreover, the Indian technology services industry has also made a strong pitch against mandating local data storage.

The temperature has been further raised recently with a speech given by Reliance Industries Limited at the Vibrant Gujarat Summit in January 2019 who was quoted as saying "For India to succeed in this data driven revolution, India needs to control its own data, must be localised, not colonised".[43] Indeed, the analogy went further with a declaration that Indian data stored overseas should be repatriated.

But what are the issues under discussion? Requiring businesses to keep a copy of data sourced from India on a server in India may present logistical issues requiring a significant improvement in the quality and quantity of data storage infrastructure. However, we believe that this is far from insurmountable so long as de-identified Big Data and metadata can be transferred freely.

The Ministry of Electronics and Information Technology recently outlined an approach to localisation which involved classifying data into three "buckets". The first bucket of data related to personal and national security would be subject to "hard localisation" (not permissible to transfer out of India); a second bucket of personal and commercial data from which portable metadata could be derived via APIs (subject to mirroring where at least a copy of the original data must exist on server in India regardless of where it is transferred there after); and, a third bucket of data deemed non sensitive and not subject to localisation.

Sources

42. The Global Services Coalition, "Data Localization Requirements in India's draft Privacy Law and Reserve Bank of India Circular on Electronic Payments", 2018
43. Medianama, "Indian data should be owned by Indians, not corporations", 2019

It is an established principle that certain data is subject to "hard localisation" in many jurisdictions. Most of the information that business use is in the form of metadata, big data, and anonymised data which can still very much be transferred through modern data infrastructure to enable business and innovation development. Businesses in large part do not want to know about "you", rather they want to know about what you do so they can service the client or customer better. Moreover, much of the modern data infrastructure already facilitates localisation of "raw" data involving physical and virtual servers maintained by established cloud computing providers working within the locally regulated frameworks.

Given the scale of India's data cache, there is already significant incentive to strengthen this infrastructure. The Asia-Pacific region will be the fastest growing data center region in the world in the next five years and much of this will be driven by India, which is currently the second-largest market for data-centre infrastructure in the Asia-Pacific after China, and predicted to be worth $7 billion by 2020.[44] Such a provision is clearly designed to boost India's domestic data centre infrastructure and industry to take poll position. Indeed, the Indian market is already unique in this regard due to its rapid adoption and growth of cloud-based storage infrastructure such as IaaS and PaaS.

This would still enable UK businesses to transfer personal data across borders and in fact opens an opportunity to collaborate in delivering the necessary data-infrastructure India will need. As such, it is premature to make judgements on data localisation. There is much detail which has to be clarified within the proposed legislation and regulatory framework. The draft Bill and its provisions should be subject to further discussion and engagement with industry practitioners both in India and internationally.

Should a bucket-based approach be confirmed, this could offer reassurance. However, important questions still remain as to what criteria will determine the data's classification, who will set and decide against this criteria, and how this will be put into practice across both sectors and borders?

It is understandable that some personal data is highly sensitive, such as biometric information and health records for instance, and should have some sensible regulatory standards for secure processing and transfer. Despite the proposal of a draft 'Healthcare Data Privacy and Security Act' 2018 recommending important safeguards, this sets precedent for separate but overlapping rules and regulations according to sector.

Regulating individuals' data differently according to sector instead of agnostically regulating the system as a whole can also create unnecessary difficulties in enforcement, ensuring a long-lasting regulatory approach, and ease of doing business.The risk of taking this approach is that enforcement becomes a complex matrix of 'buckets' and sectors that will quickly become

Sources

44. Cushman and Wakefield, "India Poised for Massive Data Center Growth", 2018

outdated and for which Indian authorities do not have the infrastructure to deliver.

Ultimately, the role and approach of the DPA will be crucial in establishing a balanced approach to data localisation. Too strict and complex an approach could lead to increase the costs and the burden of compliance on both small and large firms. This could make them less competitive globally inhibiting indigenous innovations and start-ups.

Given reassurances on the adequacy of infrastructure and an intuitive approach to data localisation encompassing clear, consistent, and limited types of data, the localisation provision should not pose a major barrier to UK businesses processing Indian personal data.

5.3 A POWERFUL STATE EXECUTIVE

Both the 'lawfulness of processing' and the 'exemptions' provisions are somewhat unique amongst large liberal nations. In that in its current form, it allows the Government to access personal data in the interest of national security without significant safeguards.

The draft Bill has a clause stating that data processing is justified where necessary to carry out any function of the Parliament, State Legislature and certain State functions.[45] However, where GDPR encompasses similar exemptions, it also includes checks and balances in the form of recital 50, mitigating most of the issues of misuse in this instance which the draft Bill does not.

Without proper checks and balances, this exemption, could pose a serious threat to the right to privacy through the potential for Government access to personal data, particularly given India currently lacks a robust surveillance framework necessary to adhere to the precedent of '*PUCL vs Union of India*'.

In particular, the 'exemptions' provision framework would concentrate significant 'national security' powers in the hands of the executive who, in the Bill's current form, would be able to initiate and review surveillance without a court order, any form of third-party review, or notification to the principal.[46]

Given that globally, the Government is as much, if not more often, a source of data misuse than businesses, this 'Executive review' approach fails to find favour in most democratic societies with strong preference toward legislative oversight or judicial approval or both. This is necessary to provide checks and balances on the Government, particularly in India where pioneering use of data and AI is transforming both State and General election campaigns.

This concern is all the more imperative given the proposed structure of the DPA.

Sources

45. Personal Data Protection Bill, 2018, Article 13
46. Council on Foreign Relations, "Three problems with India's Draft Data Protection Bill", 2018

5.4 ENSURING A STRONG AND INDEPENDENT DATA PROTECTION AUTHORITY

Ensuring a strong, independent Data Protection Authority that is tech-savvy, fairly funded and works with businesses will be critical to checking the State's power, engendering trust, and ensuring the continued relevance of data protection regulation.

Whilst the governing structure of the DPA appears robust in principle, in practice the Government will have significant influence over the members proposed by the Select Committee. This alongside the automatic membership of the Cabinet Secretary, may expose the DPA to considerable political influence, reinforcing executive power in India's data governance.

This also raises wider questions over the proposed structure of the DPA and whether businesses delivering technological innovation will have an equally meaningful say in how the sector is governed beyond vague provision for 'stakeholder consultations'. This is important as there are already concerns that the DPA's as yet vague mandate is in fact adding to barriers tech start-ups face.

In practice, the DPA will be the body interpreting the guidelines for which data requires consent and which is exempt. This includes interpreting whether businesses or Government will be able to access 'critical' non-observable biometric information, medical and mental health conditions, information relating to sexual orientation, and financial information, which, as mentioned, needs appropriate, transparent, and strong safeguards to access and processing.

Therefore, the DPA likewise needs to be equally strong, independent, and confident as to data trends and its potential misuse.

Effective data governance requires both building a close relationship with data practitioners, and ensuring sufficient structural flexibility that enables enforcement to adapt to innovation. Only governance embedded in the very methods AI uses will be sustainable and enforceable.

This requires not only a systematic, rather than sectoral, approach to regulation, but also an India DPA, which is in regular and permanent communication with foreign DPAs to ensure regulation is consistent and effective when following data across borders. Indeed, UK Information Commissioner, Elizabeth Denham, stressed that "it is important that data regulators talk to one another".[47]

The DPA also appears to have both the responsibilities of a regulator and enforcer, which poses a structural conflict of interest unless carefully designed and demarcated such as in EU Member State DPAs. The fixed penalties provision in the draft Bill is particularly problematic to achieving this. Whilst

Sources

47. UK Information Commissioner, Elizabeth Denham, speaks to the India-UK FutureTech Festival in Delhi, 2018

in theory putting fines outside the political influence is very much welcome. However, given that the DPA is to be funded through the fines it collects, it has a strong incentive to set what are disproportionately high fines to not only appear tough, but to fund its operational capacity. Though there is current no precedent for separating regulatory and enforcement responsibilities within existing Indian regulators, establishing a new DPA provides this opportunity to introduce international best-practice.

Perfect compliance by businesses would be ideal, however this would significantly damage the income of the DPA and its subsequent capacity to enforce the law, which provides the regulator incentive to abuse the penalty provision. Full funding by Government would also present further potential conflicts of interest between its ability to hold Government use of data in check and secure future funding no subject to political interference. The most sensible model in this scenario is regulatory funding secured through levies on the largest server-based businesses and organisations most closely subject to regulation.

This, coupled with a clearer mechanism for liaising with business, could go a long way towards fostering an environment of trust amongst businesses who are equally subject to, and victims of, malicious data breaches regardless of the painstaking protections they put in place.

6. WHAT DOES THE BILL MEAN FOR UK-INDIA COLLABORATION AND TRADE?

In this section we evaluate what the proposed draft Personal Data Protection Bill means for realising collaboration and innovation through a UK-India Common Data Agreement (CDA). Key to establishing a CDA is ensuring there is enough convergence in standards to minimise the gap in access, transfer, and security.

6.1 ALIGNING THE 'ADEQUATE' AND 'APPROPRIATE'

The transfer of personal data outside the UK is prohibited under the GDPR unless that country is deemed to provide an adequate level of protection and has applied appropriate safeguards to put this in place. Given that the UK is committed to continuing with its current GDPR framework for the foreseeable future, India's draft Data Protection Bill makes the transfer of personal data between the UK and India a realistic prospect for the first time.

Furthermore, as the draft Data Protection Bill outlines, this expectation works both ways - India will rightly be reluctant to transfer from its immense data cache it holds unless equal protections and safeguards are in place elsewhere.

Whilst metadata may already be traded and transferred internationally - it is the processing of large quantities of de-identified or anonymised data that truly enables machine learning and AI advances. This is particularly the case in the field of healthcare where the ability of AI to describe, predict, and prescribe access to de-identified personal data in order to learn. Secure, consensual access to identifiable data is necessary to apply this to the patient at hand.

Whilst there are clear differences between the UK's GDPR framework and India's draft Data Protection Bill on the right to confirmation and access, the right to be forgotten, automated processing, and data breach notifications which may create logistical challenges to implementing an agreement, it is clear that the draft Bill's framework, subject to clarification and implementation, meets the necessary standards of adequacy and appropriate safeguards to meet each others data transfer provisions.

6.2 ABILITY TO NEGOTIATE TRUST

Perfect convergence between national data protection regulation is unlikely to occur globally despite evidence suggesting some movement towards a broad rights-based approach. However, after placing the Bill in a global context, it is clear that underpinning India's proposed Bill is enough of a liberal, rights-based approach to data protection that makes it, in principal, fundamentally compatible with the UK's GDPR approach.

Therefore, the differences that exist between the rights and provisions afforded under the UK's GDPR and India's draft Bill are far from insurmountable, though need to be addressed.

From the perspective of India's draft Bill, negotiating a CDA that fulfils the provisions for lawfulness of processing, rights to be forgotten, to confirmation and access, automated processing, and data breach notifications appear to be comparatively straightforward as the Government of India and the DPA effectively act as the custodians of appropriate personal data use. Given that a CDA would need to be negotiated at the Government-level, this means the Government is well positioned to judge whether the UK's treatment of Indian personal data meets its criteria.

However, given the autonomy of individuals over their own data under the UK's GDPR, the UK Government is not afforded the same negotiating position. In the short-term, this will require technical solutions for the protection of individual rights of UK personal data used in India. This could include an extra transfer enabling clause in standard data consent agreements with the data principal.

In the long-term, the UK should review the GDPR. Many of the provisions that act as practical barriers to securing a UK-India Agreement, act as barriers to businesses and innovation within the UK.

Given the UK's current commitment to the GDPR in to the foreseeable future, for both countries to reach an agreement on a CDA, both must negotiate how to handle dispute resolution and requests by citizens to access, amend, or repeal their data from use by companies. Under the current draft Bill, dispute resolution will be taken through a dedicated tribunal with access to appeals through an adjudication panel. Establishing an independent tribunal and adjudicator mechanism would go a long way to resolving both domestic and international individual data disputes in an open, efficient, and accessible manner. However, the effectiveness of such dispute resolution mechanisms require the availability of highly-qualified data experts who are not yet readily available on the scale needed.

In negotiating a CDA, it should not be forgotten that both Governments would be negotiating a system that maintains the trust of citizens and businesses alike. Successfully pioneering such an agreement initially in a specific sector, such as healthcare, could go a long way to establishing the trust necessary to underpin wider CDA across other sectors.

Healthcare is a clear choice in which to first approach a negotiated agreement. Though medical records are extremely sensitive data, both regulatory approaches look set to afford patients strong rights of consent over their data. Furthermore, the potential application of data and AI to transforming healthcare are well defined and would represent the largest possible impact on the most possible lives across both the UK and India. A sensitive and sensible approach to negotiating a CDA in health data is not only possible under India's draft Bill, but could showcase the possibility to such a pioneering agreement.

7. RECOMMENDATIONS

7.1 RECOMMENDATIONS FOR INDIA'S PERSONAL DATA PROTECTION LEGISLATION

In evaluating the Indian draft Personal Data Protection Bill 2018 in light of business needs, existing approaches to international data protection, and India's own AI ambitions, we believe make nine recommendations to strengthen and enhance the Bill's ability to minimise data misuse whilst maximising India's unique data opportunity.

1. **Clarify when 'harm' leads to notification:** Definition needs to be given on what 'harm' to the data principal justifies them being notified of a data breach. To ensure that notification of breaches are not manipulated for political gain, strong assurance and clear guidelines need to be put in place making the notification procedure by the DPA fully independent, transparent and accountable.

2. **Efficient dispute resolution:** Resource and expertise should be committed to ensure that the provision for seperate tribunals to hear disputes between data principles and data fiduciaries, as well as further adjudication panels to hear appeals, have the capacity to operate efficiently and effectively. Significant investment needs to be made into fostering data expertise to ensure cases are heard fairly by qualified professionals.

3. **Clear, limited, and intuitive data localisation:** Explicit reassurance that significant data localisation will only apply to sensitive data important to an individual's personal identity or national security. The free flow of metadata and de-identified Big Data is integral to delivering innovation and India's AI ambitions.

   If a 'three bucket' approach to data localisation is taken, there needs to be clear, limited, intuitive parameters for this set out in legislation that apply to the data system as a whole, and not distinct by sector. A sector-bucket regulatory matrix places barriers in the way of data transfer and business adaptation, whilst intuitive guidelines may engender trust from businesses and individuals alike. These should be regulated in practice by the Data Protection Authority within the parameters set out in legislation.

4. **Define and support architecture and infrastructure for localisation:** The Data Protection Authority should outline what acceptable forms and formats data should take to meet the localisation provisions. Increasingly data storage makes borders difficult to distinguish in data. Where this

requires significant development in the architecture and infrastructure available to support this localised data, the Government should commit funding and collaboration to deliver this.

5. **Move exemption powers to the Legislative:** The 'exemptions' provision framework would concentrate significant 'national security' powers in the hands of the executive who, in the Bill's current form, would be able to initiate and review surveillance without a court order, any form of third-party review, or notification to the principal. This power should be moved in line with other liberal data protection regimes to the hands of the Legislative.

6. **Separate the regulator from the enforcer:** Pioneer international best-practice through a clear and comprehensive separation of regulatory and enforcement powers in India either within a single Data Protection Authority or spread out across separate, new regulatory, and enforcement authorities to avoid potential conflicts of interest.

7. **A fairly funded regulator:** The regulator should be funded through consistent and protected levies on the organisations it directly oversees that enables the regulator to build an operational capacity independent of enforcement and penalties. This will avoid regulation in the interests of the individual and businesses.

8. **A truly independent regulator:** Appointments and removals of people to or from the Data Protection Authority governing board should be based on tech savviness and experience. Appointments to and from the Board should be recommended by a truly independent committee without Government influence.

9. **A tech-savvy and sustainable regulator:** For the Data Protection Authority to be able to regulate at the pace of technological innovation, it needs strong communication with the technology practitioners themselves. This means establishing clear and permanent dialogues with both business stakeholders and foreign data protection authorities. Both in the process of drafting and implementing a final Personal Data Protection Bill, both Indian and foreign business should be consulted to ensure the most effective, innovation-oriented, outcome.

7.2 RECOMMENDATIONS FOR A UK-INDIA COMMON DATA AGREEMENT

If these moderate recommendations are incorporated into India's final Personal Data Protection legislation, there is a clear case to be made that India provides the adequate protection and safeguards necessary for a UK-India Common Data Agreement facilitating the creation of a joint 'Data Garage'. This Agreement would be pioneering and set the UK and India as world leaders in AI and data. Towards achieving this, we recommend the following:

1. **Prioritise a Common Data Agreement**: We recommend that proposals making the case for a UK India Common Data Agreement (CDA) become a priority for the UK-India Tech Partnership to enact. This CDA should include:

    a. Enabling both countries to pool and transfer de-identified and anonymous big data freely with equal access for both the UK and India, each recognising the others data protection 'adequacy' and 'safeguards'.
    b. Building shared infrastructure to house a polled 'Data Garage', which UK and Indian businesses, universities, charities, and authorities could access for the benefit of both country's AI strategies.
    c. Using sandbox protocols to encourage sharing and innovation. Underlying this is should be freedom of access and movement of metadata and datasets to foster that technological innovation environment.
    d. Such a 'data garage' should be located out of the proposed 'National Centre for Artificial Intelligence' and its network of Centers of Excellence. This would fulfill localisation requirements and India's strategy to be a hub of tech solutions as well as hone the UK's global position as a leader in AI innovation and research.

2. **Take the first step towards a CDA in Healthcare**: If necessary to test the potential scope and practical implementation of a full CDA, the UK-India Tech Partnership should propose launching a first stage of the CDA in healthcare.

3. **Enhance and expand cluster to cluster partnerships:** Cluster to cluster partnerships between the UK and India should be expanded to include leading States in technology such as Telangana and West Bengal as well as current partnerships with Maharashtra and Karnataka.

8. CONCLUSION

In this report we find that there is a unique and unparalleled opportunity for our Government's to pioneer a Common Data Agreement facilitating transformative business innovation in AI.

If the UK India Tech Partnership steps up to prioritise such an agreement, businesses on both sides are well placed to take full advantage of our complimentary AI expertise, data wealth, and ambition. This will see the UK and India become world leaders in their respective tech-fields and chart a course for each to fulfill their AI strategies and potential.

The crux of whether this is feasible, however, rests with the final shape of India's draft Personal Data Protection Bill. Having evaluated the provisions of the Bill against the needs of businesses, existing global data protection frameworks, and the necessary prerequisites of forming a CDA, we believe there is reason to be cautiously optimistic.

India's proposed Bill adopts important liberal principles towards individual data protection that makes it, in principle, compatible with the UK's GDPR approach. The devil is therefore in the detail.

Subject to important clarifications on clear, limited, and intuitive data localisation, assurance on the independence and fair funding of a Data Protection Authority with unambiguous distinctions between regulatory and enforcement roles, a streamlined dispute resolution mechanism, and shifting political checks and balances from the executive to the legislative body in line with most liberal democracies, we are confident that this could be a business and innovation enabling approach to data protection.

At its core, the Bills framework is one of qualified consent and qualified access that largely overcomes the unenforceable, innovation dampening provisions of the GDPR whilst still ensuring that initial consent is sought from the individual with systemic, ethical criteria for addressing data bias and misuse.

If the recommendations of business, as set out in this report, are acted upon, this gives us optimism that data protection in India and the UK will meet each others criteria for adequate protection and safeguards necessary for Big Data transfer between the two countries.

Big Data is the lifeblood of 21st century business. Having set out a clear path for the UK and India to deliver the fourth industrial revolution globally, we in the business community eagerly await our Government's response to this call to action.

9. GLOSSARY OF KEY CONCEPTS

Electronic and non-electronic data

The provisions of both the draft Bill and GDPR extend beyond the realm of electronic data. The draft Bill also extends to personal data in non-electronic form defining it as data that "includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means".

Personal data, Anonymous data, and De-identified Data

Both GDPR and the draft Bill apply to personal data and not to anonymised data, defining personal data as data on an individual who is directly or indirectly identifiable. Anonymised data navigates this by irreversibly transforming individual data so that it is non-identifiable.

This is different to de-identified or pseudonymised data where personal identifiers have been removed, masked, or replaced with unique but fictitious codes rendering it incapable of identifying the data principal. De-identified data, however, is still regulated due to the risks of it being re-identified.

The level of data protection requirements depends on the degree of data identifiability meaning care must be taken while anonymising personal data to ensure compliance.

Big Data

Big data is used to describe extremely large datasets that can only be analysed through computers and technology to reveal patterns, trends, and associations. This particularly relates to overarching patterns of human behaviour and interactions with other people, goods, and services. The term "Big Data" has been used to describe data in the petabyte range or larger. A shorthand take depicts big data with 3Vs -- volume, variety and velocity.

Internet of Things (IoT)

The Internet of Things is a network of devices that use embedded software to connect, interact and exchange data with other devices whether that be a mobile phone app or monitoring an aeroplanes performance.

It is an important tool for live development processes including the use of customer feedback, social media, and monitoring patterns of product usage in order to improve existing products, develop new products, and adapt production processes.

Application Programming Interface

An application programming interface (API) is a set of tools digital programmers use to build software. It is a set of clearly defined definitions, protocols, and methods of communication among various components. A good API provides all the components necessary to easily develop a program or algorithm. An API may be for a web-based system, operating system, database system, computer hardware, or software library.

An API specification can take many forms, but often includes specifications for routines, data structures, object classes, variables, or remote calls. POSIX, Windows API, and ASPI are examples of different forms of APIs.

Metadata

Metadata is data about data, summarising the various characteristics of the data concerned. Metadata for a computer image for example will consist of the image size, resolution, geo-tagging details, file format, and colour spectrum

Being able to access metadata enables the data fiduciary to comply with data protection laws by helping them to understand where the necessary data originates from; how it is being processed; where it flows to and from, and with whom it is being shared.

Databases cannot be managed, queried, or even governed without using metadata which is resource-intensive for businesses.

Cloud

The cloud is simply another form of data storage. Rather than storing and accessing, data, files, and programmes, on a computer hard drive, this can be done over the Internet via servers held by internet companies. In many ways, the cloud is a metaphor for the Internet.

10. ACKNOWLEDGEMENTS

In drafting the content of this report, the UK India Business Council would like to acknowledge the many businesses and industry experts that contributed to and reviewed our drafts, giving us insight crucial to delivering this final piece.

This report drew on discussions which took place across the India UK FutureTech Festival in Delhi, December 2018 in which we held a televised session on 'Data: The Foundation of Intelligent Economies'. We are thankful to the UK Department of International Trade for facilitating our session and the wider FutureTech Festival.

We would also like to thank our research partners, the Pahle India Foundation (PIF), who carried out in depth analysis into the provisions of the Data Protection Bill, in particular PIF Fellow, Gunja Kapoor, and former PIF Research Associate, Prithu Sharma.

PAHLE INDIA FOUNDATION
FACILITATING POLICY CHANGE

The Pahle India Foundation is a not for profit policy think tank, established in 2013 by Dr. Rajiv Kumar. PIF's motto is "Facilitating Policy Change". At PIF, they undertake research and disseminate its findings to contribute to the necessary paradigm shift in development thinking and practices in India. PIF is committed to enriching the public discourse and also to influence policy formulation that will help India successfully complete its triple transition in economic, political and social fields. PIF currently has an analytically strong team of dedicated researchers who are self-motivated. This highly qualified team specialises in analysing India's political economy and its engagement across verticals that are relatively underworked areas that will permit PIF to create a niche for itself in the research and think tank space in the country.

Authors
Richard Heald, OBE – UKIBC Group CEO
Meghna Misra-Elder – UKIBC Sector Manager - Healthcare, Digital, and Technology
Oliver Rice – UKIBC Policy and Communications Manager
Bharat Raghuvanshi – UKIBC Senior Consultant - Policy and Communication

Designed by
teammagenta

UK INDIA
BUSINESS COUNCIL

WHO ARE WE?

The UK India Business Council believes passionately that the UK-India business partnership creates jobs and growth in both countries. Through our insights, networks, and policy advocacy, we support businesses to succeed.

GET IN TOUCH

UK INDIA BUSINESS COUNCIL LONDON
12th Floor, Millbank Tower
21-24 Millbank London SW1P 4QP
enquiries@ukibc.com
Tel: +44 (0)20 7592 3040
+44 (0)800 0196 176

UK INDIA BUSINESS CENTRE MUMBAI
Trade Centre G/F & 1st Floor,
Bandra East,
Mumbai,
Maharashtra 400051
enquiriesindia@ukibc.com

UK INDIA BUSINESS CENTRE BANGALORE
Concorde Towers, UB City,
1 Vittal Mallya Road, Level 14 & 15,
Bengaluru, Karnataka 560001
enquiriesindia@ukibc.com
Tel: +91 (0) 806 7590 319

UK INDIA BUSINESS CENTRE GURGAON
WeWork DLF Forum, Cyber City,
Phase III, Sector 24,
Gurugram Haryana – 122002
enquiriesindia@ukibc.com
Tel: +91 (0) 124 502 6059

DOING BUSINESS IN INDIA HELPLINE
For support call 0800 0196 176

WEBSITE
www.ukibc.com