DIGITAL TECHNOLOGY POLICY FOR INDIA'S USD 5 TRILLION ECONOMY
DIGITAL TECHNOLOGY POLICY FOR INDIA'S USD 5 TRILLION ECONOMY
IAMAI is a young and vibrant association representing the entire gamut of digital businesses in India. Established in 2004 by the country’s leading online publishers, IAMAI has come to effectively address the challenges facing the digital and online industry including mobile content and services, online publishing, mobile advertising, online advertising, e-commerce and mobile and digital payments, among others. Fifteen years after its establishment, the association is one of the foremost professional bodies representing the online industry in India. The association is registered under the Societies Act, 1896 and is a recognised charity in Maharashtra. With a membership of over 300 Indian and overseas companies, and with offices in Mumbai, Delhi, Bengaluru and Kolkata, the association is well placed to work towards charting a growth path for the digital industry in India.

ABOUT IKIGAI LAW

Ikigai Law is an award-winning policy and law firm with a deep focus on the technology industry. The firm stands at the forefront of regulatory and commercial developments in the technology sector with a dedicated technology policy practice, engaging with crucial issues such as data protection and privacy, fin-tech, online content regulation, platform governance, digital competition, cloud computing, net neutrality, health-tech, blockchain and unmanned aviation (drones), among others. Representing diverse stakeholders including the government, businesses, and think tanks, the firm’s services are driven by the vision of becoming “partners for impact”.

This report is brought to you by the Internet and Mobile Association of India ("IAMAI"). IAMAI thanks Ikigai Law for its research and collaboration on this initiative.
# TABLE OF CONTENTS

**Executive summary**  02

**Section I : Building blocks**  09

- Digital connectivity infrastructure  11
- Mobile device ecosystem  15
- Digital literacy and consumer awareness  18

**Section II : Digital economy policy**  21

- Data governance  23
- Cyber security  30
- Encryption and surveillance  34
- Regulation of cloud service providers  41
- Emerging technologies: artificial intelligence and the internet of things  44
- Digital payments  50
- Platform regulation: intermediary liability  60
- Evolving issues: competition and digital taxation  64
EXECUTIVE SUMMARY

The prime minister in his first address to the new parliament laid out an ambitious plan to make India a USD 5 trillion economy by 2024. Expressing his confidence in the country's potential, he stated that while this was a difficult target, it was an achievable one.

Technology and digitisation will play a key role in achieving the USD 5 trillion milestone, as indicated by the finance minister in her budget speech for the year 2019-20. This comes as no surprise, as two of the world's largest economies have grown over the last 15 years on the back of the digital and technology industry. India's growth in this period has been driven largely by technology as well. For instance, the government's focus on the 'Digital India' programme has led India to become one of the largest and fastest-growing digital markets in the world.

This digital market will be contributing significantly to the growth of the Indian economy, as is evident from the fact that the country's existing digital ecosystems alone contribute up to USD 500 billion of economic value. As per the ministry of electronics and information technology, this number is set to rise to USD 1 trillion by 2025. Therefore, as India moves towards becoming a leading global economy, it is imperative for the government to re-look, re-boot and re-think its technology policy.

We believe that technology use and adoption is going to be the driving force of India's journey to becoming a USD 5 trillion economy. The positive externalities and the multiplier effect that digital and emerging technologies are going to bring about are going to be at the root of India's endeavours to become one of the largest economies of the world. Over and above the estimated USD 1 trillion contribution of digital ecosystems to the economy, digitisation and technology are going to play a key role in the growth of existing and new sectors of the economy. Affordable access to the internet is allowing the Indian consumer base to become well-connected with the marketplace regardless of geographic location, making room for fast-moving technology-based businesses with significant economic potential. It is estimated that at least 60-65 million new jobs could be created in this new digitally-driven marketplace.

It is our belief that a carefully crafted, deeply thought out and widely consulted set of policies that are geared towards the adoption, use and promotion of digital technology will go a long way in ensuring that we meet our targets. Such a policy will not only bring us close to the target in terms of gross domestic product ("GDP"), but will also make sure that the resource allocation needed and the proper distribution expected would also be done speedily and efficiently. We look forward to partnering with the government in its efforts to achieve this goal. We truly believe that through concerted efforts; consultative processes with multiple stakeholders including industry players, academia and civil society; and a facilitative regulatory framework, India can achieve this goal.

In this report, therefore, we present to the government, regulators, think tanks, industry and technology enthusiasts a set of guiding principles that may be used in the making of the appropriate technology policy that India needs on its way to becoming a USD 5 trillion economy with its attendant socio-economic benefits to the citizens. We hope to bring about a set of guiding principles that may be used in the making of the appropriate technology policy that India needs on its way to becoming a USD 5 trillion economy with its attendant socio-economic benefits to the citizens. We hope

---

that this report is able to assist India in actualising its digital potential, and formulating an innovation friendly regulatory framework. The report is meant to be sector-agnostic and future-ready so as to remain relevant in times when regulators are forced to play cat and mouse with new and evolving technologies. It has been divided into two sections. Section I deals with crucial infrastructural building blocks that form the foundation of the digital economy. These include India's connectivity infrastructure, its mobile device ecosystem, and the steps taken to increase digital literacy and consumer awareness. Section II deep dives into targeted areas of the Indian digital economy and suggests recommendations for strengthening them. It examines the challenges presented by the broader issues of data governance; platform regulation and intermediary liability; cyber security; encryption and surveillance; competition and digital tax, as well as the regulation of specific areas such as emerging technologies; cloud service providers; and digital payments.

A. Regulatory Approach

Guided by the foresight of the prime minister's vision for a ‘Digital India’, the government has played the role of an encouraging enabler of digital technology since 2014. In the five years since the launch of the ‘Digital India’ programme, the country has witnessed a steady rise in the growth of digital infrastructure and e-governance services, that in turn have enabled the digital empowerment of citizens across the board. These advances have complemented the government’s efforts in meeting the goals of the ‘Startup India’ initiative, which intends to build a “strong and inclusive ecosystem for innovation and entrepreneurship in India.” For instance, Indian startups have received increasing amounts of investments every year, with a total of USD 4.2 billion in funds raised in 2018, recording a 108% growth compared to the amount raised in 2017. The resolution of the ‘angel tax’ issue and tax exemptions proposed by the finance minister in the union budget speech for 2019 will further aid this growth.

The success of the ‘Digital India’ programme has had positive effects in other sectors of the economy as well. For instance, affordable access to the internet coupled with an encouraging regulatory ecosystem has allowed India to become home to the second largest number of internet users in the world. This in turn has allowed e-commerce companies to thrive. The push towards incentivising digital payments proposed under the union budget for 2019 will allow further expansion of the e-commerce sector. The government has focused on giving a push to emerging technologies as well, as evidenced by the NITI Aayog’s ‘National Strategy for Artificial Intelligence’, the National Telecom Machine-to-Machine Communications Roadmap and the draft Internet of Things Policy document. The forward-looking National Digital Communications Policy, 2018 also lays out a detailed roadmap for harnessing these technologies.

---

More of such open and encouraging policies are needed in order for India to achieve the USD 5 trillion economy target. India is a resource poor and brain rich country, and therefore our comparative advantage is not in natural resources or in finance, but in innovation in policy. We should leverage this advantage by making India the experimental ground for cutting-edge innovations in technology. India provides the ideal fertile ground for projects like the ‘HUB 71 platform’, that are currently being hosted in Abu Dhabi.

In order to make India the world leader in policy and regulatory innovation, our regulatory approach should focus on the regulation of the ‘core’ industry players, and not entities that fall on the ‘edge’ of the regulatory spectrum. This can be done by drafting clearly articulated outcome-based regulations. It is also important to make regulations that tackle real threats, as opposed to perceived challenges. This allows nascent and emerging industries to stand on their feet before being subjected to strict regulatory scrutiny. A co-regulatory and self-regulatory framework allows regulators to create such enabling rules.

India already has some experience in evolving co-regulatory and self-regulatory frameworks. For instance, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 allow companies to either follow industry best practices for data security, or frame their own codes and have them ratified by the government. The Data Security Council of India established by the National Association of Software and Services Companies prescribes best practices, codes and frameworks to enhance cyber security and privacy. In a more recent example of participative regulation, certain social media companies, acting through the Internet and Mobile Association of India evolved a voluntary code governing the takedown of online content during India’s recent general elections, and worked with the Election Commission of India on this issue.

Participative regulatory models will not only help us address emerging challenges in India’s digital economy, but will also allow us to position ourselves as a technology-friendly jurisdiction. In our view, consultative regulatory frameworks comprise clear, transparent, and effective dialogue at every stage between the government and all stakeholders; graded, context-specific, and tailored regulatory responses, as opposed to heavy-handed ones; an appetite for innovative regulatory structures such as regulatory sandboxes; and a willingness to enhance regulatory capacity and measure performance.

**B. Recommendations**

We make the following recommendations to strengthen India’s building blocks, and address key digital economy challenges across various sectors.

**Section I : Building blocks**

**Connectivity infrastructure**

1. Prioritize the adoption and implementation of the key recommendations of the National Digital Communications Policy, 2018 (“NDCP 2018”) that lays out a comprehensive roadmap to enable the adoption of new and emerging technologies in India.

---

18 Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011.
19 The Data Security Council of India, available at https://www.dsci.in/.
2. Ease licensing and regulatory requirements for telecommunications services, which will boost foreign investment and facilitate the development of next generation technologies in India.

3. Introduce structural reforms in the management of the Bharat Broadband Network Limited and other implementing agencies to improve their efficiency. This will be a decisive factor in realizing the vision for universal broadband coverage and other goals.

**Mobile device ecosystem**

1. Align various regulations governing different aspects of the mobile device ecosystem, and institute a single window compliance mechanism for the registration and testing of mobile devices to be sold in India. This will facilitate the ease of doing business for both sellers and manufacturers.

2. Simplify product testing and certification requirements for imported products. India’s current processes are expensive and time consuming for importers and manufacturers, and redundant for devices being imported from countries such as the US, that already have strict standards for exported products.

3. Create an export-focused electronics manufacturing hub in India.

**Digital literacy and consumer awareness**

1. Develop a comprehensive national digital literacy and education strategy that integrates the needs of various stakeholders, covers multiple skill clusters, and disseminates information at various levels. This strategy must also include a focus on the value to users from going digital and the difference that it will make in their daily lives.

2. Adopt a phased approach to digital literacy programs. The requirements of different demographic groups, the urban-rural divide, the end use of the digital medium, and impact on employability are factors that should be considered.

3. Educate consumers on consumer rights in the digital world and grievance redressal mechanisms for online transactions.

**Section II: Digital economy policy**

**Data governance**

1. Harmonise all government policies on data governance in line with the recommendations of the Justice Srikrishna Committee and the frameworks under the Personal Data Protection Bill, 2018, which will serve as the basis for the national law on data protection.

2. Reconsider data localisation requirements, considering the harms of data localisation to the Indian economy, and increased threats to cyber security.

3. Encourage the free flow of data across borders to ensure that Indian companies have access to the best cloud service platforms, big data analysis tools, and other emerging technologies from around the world. In parallel, focus on strengthening inter-governmental cooperation arrangements and Mutual Legal Assistance Treaties to facilitate cross-border flows of data. Additionally, focus on alternate measures (including bilateral agreements, adequacy arrangements) to address concerns relating to transfer of data.

4. Redesign notice and consent frameworks for the digital age. Traditional notice and consent frameworks lead to consent fatigue and a lack of informed consent, impair the development of new technologies, and do not safeguard data principals’ rights. Instead, accountability-based models should be adopted. Consent frameworks should ensure that the control over data remains with the data principal and is not passed on to the data processor.

5. Use the purpose of data processing as the basis for determining the sensitivity of data, instead of adopting a list-based approach.

6. Revise the classification of data under the Personal Data Protection Bill, 2018 to exclude indirectly identifiable data from the ambit of ‘personal data’. Further, the definition of sensitive personal data under the bill should exclude financial data.
Cyber security

1. Formulate implementation strategies for the National Cyber Security Policy, 2013, which will boost the development of India’s cyber security framework.

2. Encourage private sector participation in the formulation of cyber security policies. This will encourage the development and adoption of innovative and nimble solutions well-suited to address increasingly dynamic and sophisticated threats to cyber security.

3. Strengthen regulatory accountability frameworks applicable to the CERT-In by mandating and enforcing standard response procedures in response to cyber security incidents. In addition, strengthen accountability frameworks applicable to law enforcement requests for access to data.

4. Enact a robust cyber security law which will help address the rise in cyber security breaches and ensure the better implementation of cyber security protocols.

5. Reconsider data localisation requirements as storing data across several jurisdictions keeps it more secure and helps in data recovery in case of disasters.

Encryption and surveillance

1. Harmonise the various laws governing encryption and surveillance to address overlaps and conflicts and balance individual privacy, business interests, and law enforcement objectives.

2. Adopt leading industry standards for encryption in place of the standards currently prescribed under Indian law, as they do not adequately secure information.

3. Prescribe narrow and tailored grounds for decryption that balance law enforcement imperatives with individual privacy.

4. Introduce legislative or judicial oversight over government surveillance to safeguard privacy and align Indian law with global best practices.

5. Disclose law enforcement requests to impacted persons in the interests of government transparency and individual privacy.

6. Retain end-to-end encryption and do not institute encryption backdoors. While end-to-end encryption enables the freedom of expression and privacy of individuals, backdoors create cyber security vulnerabilities which may be exploited by hackers and attackers.

7. Permit bulk encryption as it provides a high degree of data and cyber security, and a ban on bulk encryption increases business costs.

8. Promote more resilient authentication processes such as risk based or multi-factor authentication to enhance transactional security.

Cloud computing

1. Allow cross border data flows as these are integral to the business models of global cloud service providers, ensuring data security, and access to innovative cloud computing services for Indian businesses.

2. Implement light touch regulation and ease the regulatory burden on cloud service providers.

3. Ensure regulatory consistency by ensuring that cloud computing is regulated only under India’s information technology laws, and not as a telecommunications service.

Emerging technologies

1. Design data governance frameworks that are well-suited for emerging technologies, re-visit traditional notice and consent models, purpose limitation mandates, and data localisation, while also addressing privacy concerns.

2. Introduce device-specific certification standards for Internet of Things (“IoT”) devices depending on their functionality, security concerns, and data collection capabilities.

3. Encourage artificial intelligence (“AI“)/machine learning (“ML“), and IoT technology adoption within the government and build regulatory capacity on these emerging technologies.
4. Promote awareness about AI/ML and IoT technologies and devices, including their security safeguards, which will also help boost consumer confidence in emerging technologies.
5. Adopt global best practices, standards and certifications for AI/ML and IoT technologies.
6. Develop an implementation roadmap in consultation with stakeholders for the National Artificial Intelligence Strategy, 2018 to give effect to its recommendations across sectors.
7. Discuss patents frameworks for AI algorithms, which are exempted from patentability under current Indian law. Reforming this position will enable AI development and prevent intellectual property theft related to AI.

**Digital payments**

1. Lower regulatory barriers to entry for new businesses by narrowly defining payment systems and regulating technology service providers differently from payment systems.
2. Adopt industry-led standards for non-systemically important payment systems that do not pose a threat to the financial market infrastructure to ease costs and increase flexibility in operations for new businesses.
3. Ease eligibility criteria for the Reserve Bank of India’s (“RBI”) regulatory sandbox framework to allow more mature start-ups and licensed payment systems to participate in the sandbox environment.
4. Relax additional factor authentication requirements for recurring transactions, in order to promote subscription-based businesses.
5. Simplify know-your-customer (“KYC”) norms for pre-paid instruments, which currently require the same level of KYC as banks.
6. Implement security by design principles that adhere to global norms for information and network security protocols to ensure robust cyber security in critical national financial infrastructure.
7. Encourage the adoption of digital payments by introducing tangible benefits including tax incentives and dis-incentivise cash transactions to reduce India’s dependence on cash.
8. Create better customer protection frameworks that will lead to better customer trust in innovative finance products by promoting multi-lingual financial literacy and a robust grievance redressal machinery.
9. Create an independent and transparent supervisory board for regulating payment systems to foster competition, consumer trust, and stability in the payments sector.
10. Promote interoperability between digital payments’ interfaces by giving impetus to the RBI’s Prepaid Payment Instruments (PPIs) – Guidelines for Interoperability.
11. Reform the National Payments Corporation of India (“NPCI”) to resolve the conflict of interest it faces as a participant in the digital payments’ space as well as a rule-making body for Unified Payments Interface (“UPI”) in India.
12. Enhance industry participation to realise the RBI’s vision for digital payments for the period 2019-2021.

**Platform regulation: Intermediary liability**

1. Preserve safe harbour protection for internet intermediaries, as safe harbours are crucial for innovation and entrepreneurship, and the freedom of expression of Indian citizens.
2. Do not introduce pro-active content monitoring requirements for internet intermediaries as they contravene the directions of the Supreme Court22, and may lead to intermediaries censoring legal content and deploying opaque, automated content filters, all of which harms free speech.
3. Do not require intermediaries to set up offices in India as these are strategic business decisions best left to market forces. Moreover, facing increased compliance costs, companies may altogether cease to offer their services in India, harming Indian consumers and businesses.
4. Do not prescribe additional regulation for content on online platforms as the Information Technology Act, 2000 and rules framed under it are sufficiently equipped to deal with the regulation of online content.

---

Evolving issues: Competition law and digital taxation

1. Incentivise the participation of technically skilled experts in the Think Tank on Digital Markets ("ThinkTank") and invest in regulatory capacity building.
2. Increase transparency in internal processes of the Competition Commission of India, the Think Tank and other committees constituted.
3. Update the Competition Act, 2002 to address issues of a growing digital economy and innovative business models, such as virtual market places.
4. Consider the introduction of settlement proceedings in line with global best practices to ensure the swifter resolution of disputes, and customised remedies for each case.
5. Apply new rules affecting taxation prospectively and clarify that they have no bearing on ongoing assessments or appellate proceedings.
6. Adopt a balanced approach to amending India’s tax framework based on in-depth consultation with all stakeholders, as these amendments will replace long-settled international norms, and have ripple effects throughout the Indian economy.
7. Honour existing Advance Pricing Agreements that the Central Board of Direct Taxes has entered into with numerous tax payers.
SECTION : I

BUILDING BLOCKS OF A 5 TRILLION DOLLAR ECONOMY
Overview

This section focuses on the fundamental building blocks of India's digital economy and assesses the progress made on strengthening each of these over the course of 2014-2019. We have identified three key building blocks, which are digital connectivity infrastructure; mobile device ecosystem; and consumer awareness and digital literacy. It is essential to strengthen all three building blocks, as they control the pace of digitisation in the country, which in turn controls the pace at which India becomes a trillion dollar economy. Policy-making for these building blocks must focus on the promotion of the underlying infrastructure and technologies, and must step in to regulate them only in case they veer off targeted goals. In this report, we have discussed these building blocks as follows:

1. Digital connectivity infrastructure, which focuses on India's telecommunication and internet infrastructure. This sub-section includes measures taken by the government to promote internet and broadband coverage.

2. Mobile device ecosystem, which focuses on India's device manufacturing capacity. This sub-section includes an assessment of the state of hardware security in the country.

3. Consumer awareness and digital literacy, which deals with the protection of consumer rights in the digital world. This sub-section also examines the steps taken to improve access to internet and introduce best practices for privacy and safety online.

These building blocks have been dealt with over the course of three sub-sections below. Each of these sub-sections sets out the context for the discussion, examines the current state of law and policy, and outlines our views on the challenges hindering the development of each building block and our suggestions to address them.
A. Context

Digital infrastructure is a "collection of technological and human components, networks, systems, and processes that contribute to the functioning of an information system". Per the Telecom Regulatory Authority of India ("TRAI"), the country's digital infrastructure includes its e-service infrastructure, information technology ("IT") infrastructure and many such components. Digital connectivity vastly impacts growth because it facilitates communication and commerce, that forms the basis of economic growth. In fact, it is reported that "a 10 per cent increase in India's total Internet traffic, delivers on average a 3.3 per cent increase in India's GDP, and a 10 per cent increase in India's mobile Internet traffic, delivers on average a 1.3 per cent increase in India's GDP." It is therefore crucial to develop robust digital connectivity infrastructure. This was also highlighted by the ministry of electronics and information technology ("MeitY") as a part of its overall vision for a 'Digital India', and the recently released National Digital Communications Policy, 2018 ("NDCP 2018"). Given their emphasis on strengthening this particular building block, the 'Digital India' programme and the key recommendations of the NDCP 2018 are the main focus of this sub-section.

B. Current state of law and policy

'Digital India', was launched with a vision "to transform India into a digitally empowered society and knowledge economy". Its goals are the development of secure and stable digital connectivity infrastructure, the delivery of government services digitally, and universal digital literacy. Digital connectivity infrastructure in turn comprises of three sub-components: (i) broadband internet for all urban and rural India; (ii) universal access to phones; and (iii) common services centres ("CSC").

---

33 The vision is to ensure that there is a massive and growing penetration of mobile phones in India, especially in rural areas, which provides a ready and widespread base for access to and delivery of public services.
34 This includes information and communication technology-enabled front-end service delivery points (kiosks) at the village level for delivery of government, financial, social and private sector services in the areas of agriculture, health, education, entertainment, banking, insurance, pension, utility payments, etc. See https://digitalindia.gov.in/content/vision-and-vision-areas#.
To realise its potential under the 'Digital India' programme, the government of India has launched several initiatives such as the National e-Governance Plan, 2006, which was relaunched in 2015 as 'e-Kranti: National e-Governance Plan 2.0', BharatNet or Mahanet, the Common Service Centre scheme 2.0, the Electronic Development Fund ("EDF"), the Centre of Excellence for the internet of things, 2015, the Digi-Locker, the Digitize India Platform ("DIP"), and the 'Single Window Interface for Trade' ("SWIT").

The NDCP 2018 is amongst the most recent and significant policy reforms for digital connectivity infrastructure launched by the Indian government. The NDCP 2018 proposes to restructure the legal, licensing and regulatory framework for connectivity and digital infrastructure in the country, including amendments to the Indian Telegraph Act, 1885 and related laws. Some of its key objectives are (i) provisioning of broadband for all; (ii) creating four million additional jobs in the digital communications sector; (iii) enhancing the contribution of the digital communications sector to eight per cent of India's GDP; (iv) enhancing India's contribution to global value chains; and (v) ensuring digital sovereignty. Some of the highlights of the NDCP 2018 are as follows.

---

35 Approach and Key Components of e-Kranti: National e-Governance Plan 2.0, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=117690. Under e-Kranti, the number of mission mode projects (projects which have clearly defined objectives, scope, implementation timelines and milestones, as well as measurable outcomes and service levels) has increased from 31 (as set in 2006) to 44. See e-Kranti electronic delivery service, available at https://digitalindia.gov.in/content/ekranti-electronic-delivery-services.


37 The Common Service Centre scheme, available at https://csc.gov.in/. It aims to establish a self-sustaining network of 2.5 lakh Common Service Centres at the gram panchayat level to deliver citizen-centric services.

38 Electronic Development Fund, available at http://www.edfindia-canbankventure.com/about-edf.php. This set up as a 'fund of funds' to provide risk capital to companies which are developing new technologies in the area of electronics, nanoelectronics and information technology.

39 Ministry of electronics and information technology, Centre of Excellence of IoT, available at http://www.coe-iot.com/. This aims to jump start the internet of things ecosystem by taking advantage of India's information technology strengths.

40 Ministry of electronics and information technology, DigiLocker available at https://digilocker.gov.in/. This is a flagship programme of the Indian government which aims to give citizens a shareable private space on a public cloud. It does so by leveraging the public cloud to make all documents readily available to users.

41 Digital India, Digitize India Platform, available at https://digitizeindia.gov.in/. The 'Digital India' platform extracts useful data from scanned images of government documents by identifying key data in every document and transcribing it into a machine-readable format.

42 Central board of excise and customs, circular no. 09/2015-Cus, dated 31 March 2015, available at https://www.icegate.gov.in/Download/Circular_No_09_2015_Cus.pdf. This acts as a single window mechanism to allow importers and exporters to seek online clearance of their documents at a single point of contact and aims to reduce interface with governmental agencies, time for approval and the cost of doing business.


The NDCP 2018 makes key observations on harmonising certification, legal and regulatory standards applicable to telecom services, spectrum, and non-discriminatory treatment of data, fibre, active and passive infrastructure sharing, data protection, and cloud service providers.

C. Recommendations

1. Prioritise the implementation of NDCP 2018 goals:

The NDCP 2018 is a forward-looking policy which seeks to create a much-needed roadmap for enabling the adoption of new and emerging technologies such as 5G, artificial intelligence, robotics, the internet of things ("IoT") and cloud computing. In order for its vision to be realised, the government must prioritise the adoption and implementation of its key recommendations. For instance, the policy recommends the development of "regulatory frameworks and incentives for promoting the establishment of International Data Centres, Content Delivery Networks and independent interconnect exchanges in India." It also emphasises the creation of enabling infrastructure for the convergence of information technology, telecommunications and broadcasting services. These are welcome steps which will provide a much-needed impetus to private sector participation in the development of India’s digital connectivity infrastructure. The government has already taken significant steps towards realising these goals. For instance, the department of telecommunication ("DoT") has constituted committees to invite the views of different ministries on the policy's objectives. This progress is encouraging and we urge the government to continue to move at this pace to ensure that the recommendations of the NDCP 2018 are implemented in a time-bound manner, as this will allow India to move closer to its goal of becoming a 'Digital India'.
2. **Reform the licensing and regulatory frameworks for telecommunications services:**

In keeping with the MeitY’s ‘Trillion Dollar Digital Opportunity’ roadmap, the NDCP 2018 aims to enable the development of next generation technologies in India by attracting “investments of USD 100 Billion in the Digital Communications Sector”. In order to realise this goal, the government must take concrete steps towards promoting the ease of doing business in India in critical sectors such as telecommunications. The NDCP 2018 proposes a number of progressive reforms for this purpose. For instance, it recommends the reduction of license and regulatory compliance requirements for telecommunications players, in keeping with international best practices. It also proposes simplifying the existing systems and procedures for the grant of licenses, approvals, clearances, permissions and the development of a comprehensive end-to-end online platform. These reforms should allow companies that are not traditional licensed telecommunications players to participate in the provision of telecom services. We recommend the adoption of a regulatory sliding scale for this purpose. This scale should apply different regulatory approaches to different categories of players, depending on the level of risk posed by these players to national security, privacy, law enforcement and foreign relations. For instance, companies that are involved with critical aspects of telecommunications, such as the management and use of active infrastructure, can continue to be subject to a licensing framework, while companies involved with the provision of relatively low-risk services can be allowed to engage with the provision of telecommunications services subject to light touch regulation or registration models.

3. **Improve the efficiency of implementing agencies:**

One of the key goals of the NDCP 2018 is the promotion of “Broadband for All” for accelerating socio-economic development. It recommends establishing a national broadband mission for this purpose. The ability of agencies like Bharat Broadband Network Limited to function efficiently and effectively will be a decisive factor in the realisation of the desired results under the NDCP 2018. The government should consider initiating a structural overhaul to bring in professional management and expertise at both the planning and implementation levels in order to ensure that this is taken care of.

---


MOBILE DEVICE ECOSYSTEM

A. Context

India is the second largest market for smartphones in the world. In 2018, smartphone shipments to India reached 33.5 million, growing by 19.8 per cent year-on-year. Some reports indicate that electronics imports have exceeded gold imports to become India's second largest import category, after oil.

The value share of the mobile handsets industry in the total electronics segment in India is estimated to be nearly 35 per cent, which makes the mobile handsets industry the largest electronics vertical in the country. India now has 120 units manufacturing mobile phones compared to two units in 2014. Out of these, about 59 units are producing mobile handsets while the rest of them are engaged in manufacturing various components of mobile handsets, such as chargers, adapters, battery packs, wired headsets, and other mechanical parts. Around 225 million mobile handsets were manufactured in India in 2017-18 compared to 60 million in 2014-15. In value terms, the industry stood at USD 20 billion in 2017-18 compared to USD 2.99 billion in 2014-15. In volume terms, production grew to about 175 million in 2016-17 over 110 million in 2015-16, exhibiting a growth of about 60 per cent.

These numbers explain why a number of government schemes, policies and incentives in the recent past have prioritised the development of electronics manufacturing, and in particular the manufacturing capacity of the mobile devices industry in India. The aim has been to prepare India's readiness as a global mobile device manufacturing hub, with the hope of attracting takers for its potential export capacity in the near future.

B. Current state of law and policy

Over the years the government has taken several steps to promote the domestic manufacturing electronic device industry such as the introduction of the Modified Special Incentive Package ("M-SIPS"). The scheme mainly provides subsidies for investments in capital to the tune of 20 per cent for investments in special economic zones ("SEZs") and 25 per cent in non-SEZs. Similarly, the Phased Manufacturing Programme ("PMP") was launched with the objective of promoting the indigenous manufacturing of mobile devices and its sub-parts/components.

The value share of the mobile handsets industry in the total electronics segment in India is estimated to be nearly 35 per cent, which makes the mobile handsets industry the largest electronics vertical in the country.
This programme introduces differential excise duties for domestic mobile manufacturers, which provides an impetus to the domestic industry. Under the PMP differential excise duty dispensation, excise duty was enhanced to 11.5 per cent in favour of domestic cellular mobile handset manufacturers vis-a-vis imports in the Union Budget 2015-16. In February 2019, the Union Cabinet approved the National Policy on Electronics, 2019 ("NPE 2019"), which seeks to position India as a global hub for electronic system design and manufacturing ("ESDM") by encouraging the manufacture of core components of electronic devices.

As per a recent press release from the ministry of commerce & industry, there are 127 manufacturing mobile handsets in the country and all of them are operating from the domestic tariff area ("DTA"). As they are operating from the DTA, they enjoy the benefits (in addition to the incentives under the SEZ Act, 2005 & SEZ Rules, 2006) of a rationalised tariff structure under the PMP, availing benefits under the M-SIPS. Additionally, one hundred per cent foreign direct investment is permitted for the manufacture of mobile handsets and their sub-assemblies and nil basic customs duty is imposed on specified capital goods for the manufacture of mobile handsets. The government has also set up an EDF with a corpus of USD 320 million to provide risk capital for start-ups planning to develop new technology in electronics, nanoelectronics and information technology.

As for the sale of devices, the Electronics and Information Technology Goods (Requirement for Compulsory Registration) Order, 2012 ("Registration Order"), requires anyone who sells, imports or distributes devices to conform to the standards specified in the Registration Order. This specifically covers mobile phones, power adapters for IT equipment, power adapters for audio, video and similar electronic apparatus, sealed secondary cells and batteries containing alkaline or non-acid electrolytes for use in portable applications. In addition, MeitY also conducts surveillance of these goods to curb the sale of non-registered/non-compliant goods in the domestic market.

C. Recommendations

1. Align various laws governing the device ecosystem:

Presently, there are a number of different laws and regulations governing the device ecosystem. Aligning all these requirements under one comprehensive umbrella scheme can greatly help with the ease of doing business, for both manufacturers and sellers of such devices. In particular, we recommend the establishment of a single window compliance mechanism for the registration and testing of mobile devices that are to be sold in India.

---

2. Simplify product testing and certification requirements for imported products:
At present, once a mobile device is manufactured or imported into India, it has to go through a number of agencies and regulations to be tested, certified and approved before it can enter the Indian market. Manufacturers and/or importers are thus required to incur significant costs for selling products in India, since these processes are expensive and time consuming. This can be especially cumbersome for the import of mobile devices from countries with higher standards of testing and certification (such as the European Union and the US), which already have strict standards of testing and certification for exported products. The existing regime in India requires the certification and approval of such devices in India again before they are allowed to sell in the Indian market84. This creates redundancies and inefficiencies. Therefore, the existing regime should be modified to simplify the certification and approval requirements of mobile devices85.

3. Create an export-focused manufacturing hub in India:
The growing digital economy has driven the demand for electronic products in India, which is expected to rise to USD 400 billion by 202586. In order to meet this increasing demand, the NPE 2019 recommends the creation of a globally competitive domestic electronics manufacturing hub in India, with a special emphasis on exports. This is in keeping with the government’s ‘Make in India’87 vision and will enable India to become a global leader in the electronics manufacturing services segment. Therefore, the recommendations of the NPE 2019 must be implemented on a priority basis.

---

DIGITAL LITERACY AND CONSUMER AWARENESS

A. Context

In a country that is yet to achieve universal adult literacy, one may wonder as to why digital literacy should be considered important. The reason is simple: the number of active internet users in India is staggering. As of June 2018, the number of internet users in India was at 500 million\(^8\). This number is expected to reach 627 million by the end of 2019. Thus, it is evident that the country is witness to an astounding growth of its digital population.

While our accelerated digital growth is laudable, we cannot ignore the acute urban-rural divide which is an integral part of this growth. While urban India already has 295 million people using the internet, only 186 million Indians from rural India currently use the internet, even though it comprises a much larger share of the entire country’s population\(^9\). Of the 295 million internet users in urban India, the largest share comes from the top nine cities of the country\(^10\). This context is important for understanding the impact of the digital literacy initiatives that have been discussed below.

B. Current state of law and policy

Digital literacy

The digital literacy policies that are currently being implemented within India fall under the ‘Digital India’ initiative. ‘Universal digital literacy’ is a key goal under this initiative\(^11\). It requires that at least one person should become e-literate in every household such that citizens have the ability to fully exploit digital technologies to empower themselves; and seek better livelihood opportunities to become economically secure.

The Pradhan Mantri Gramin Digital Saksharta Abhiyan or the National Digital Literacy Mission (‘NDLM’) scheme is another core part of the ‘Digital India’ initiative\(^12\). The NDLM, which focuses on rural communities\(^13\) has been formulated to “impart IT training to 52.5 lakh persons, including Anganwadi and ASHA workers and authorised ration dealers in all the states/union territories across the country …”\(^14\). This is meant to ensure that citizens are IT literate, so that they can operate digital devices, send and receive emails, and search the internet for information. It also enables citizens to effectively access the different e-Governance services being offered by the government and other agencies\(^15\).

---


\(^11\) Ministry of electronics and information technology, Digital India, vision and vision areas, available at https://digitalindia.gov.in/content/vision-and-vision-areas.


\(^14\) The National Digital Literacy Mission is primarily focused on rural communities and citizens from the lower income groups as the eligibility criteria is non-information technology literate, illiterate and up to 7th/8th standard pass. This information is available at http://nielit.gov.in/calicut/content/national-digital-literacy-mission-ndlhm.

In 2019, the Ministry of Human Resource Development ("MHRD") released the National Education Policy, 2019 ("NEP")96, which covers elementary education for colleges in both rural and urban India. This policy acknowledges that there is a need to reorient the content and process of school education to include several factors including digital literacy. On the issue of digital literacy, the NEP provides that the "new curriculum will integrate digital literacy for all learners at the basic level, keeping in mind the available digital infrastructure on the ground"97. Additionally, in order to integrate digital devices and the use of IT within the existing education system the government of India launched e-Basta in July 2015, which creates a framework for making school books accessible in the digital form as e-books to be read and used on tablets and laptops98.

Protection of consumer rights

Diverting resources towards increasing digital literacy must be accompanied by a commensurate effort towards tackling the issue of protecting consumer rights in the digital space. This is addressed by the proposed the Consumer Protection Bill, 2018 ("CPB, 2018"). Unlike the Consumer Protection Act, 1986 ("CPA, 1986"), which does not make any express reference to online consumer or e-commerce transactions, the CPB, 2018 explicitly protects digital consumers99. It also accounts for unfair trade practices that can occur through e-commerce transactions and electronic service providers. This is a welcome step forward, since it leaves no room for ambiguity on the issue of the applicability of the CPB, 2018 in the digital sphere.

C. Recommendations

1. Implement a national digital literacy strategy:

Digital literacy is an umbrella concept that covers different ‘skill clusters’100 such as computer literacy, information communication technology ("ICT") literacy, information literacy, and media literacy101. A robust digital literacy program, which is effectively implemented, will ensure that there is awareness and protection of consumer rights. Therefore, there is a need to develop a national digital literacy and education strategy which takes into account the fact that there is a need to integrate the requirements of a variety of stakeholders and disseminate the information at various levels. In this context, it is important to remember that there is no “[O]ne-size-fits-all assessment of digital competence that can serve all purposes and contexts”102.
2. Approach digital literacy in a holistic manner:

The digital literacy policies and programmes implemented in India at present focus primarily on the rural population and hence primarily on integrating computer based learning and digital skills. We need to look at digital literacy in a more holistic manner. The definition of the term ‘digital literacy’ adopted by the Global Alliance to Monitor Learning (“GAML”) summarises it well: “digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life”103. Therefore, there needs to be a more integrated approach in dealing with this issue. A phased approach which looks at the distinct requirements of the different target demographic groups, types of population (urban and rural), end use of the digital medium, and impact on employability may helpful in devising a pragmatic and sustainable approach.

3. Address lack of awareness regarding grievance redressal procedures:

On the issue of consumer rights, the CPB, 2018 is a step in the right direction, as it takes into account the existence of the digital consumer. There is also a lack awareness of grievance redressal mechanisms for online transactions and the manner of enforcement of consumer rights. This coupled with the high rate of cybercrimes comes in the way of ensuring continued growth of digital penetration in India. We recommend encouraging public-private partnerships to create more awareness on the routes for grievance redressal to remedy this problem.

SECTION : II

DIGITAL ECONOMY POLICY
Overview

This section focuses on key areas in the digital economy policy ecosystem to assess the status quo and identify challenges that need to be addressed, and offers recommendations to tackle these. We have identified eight priority areas, namely, data governance, cyber-security, encryption and surveillance, cloud computing; emerging technologies, digital payments, platform regulation, and evolving issues relating to competition law and digital taxation. Each of these areas is a critical part of the digital economy, the growth of which is vital for the realisation of the Prime Minister’s vision of a USD 5 trillion worth Indian economy. In this report, we have discussed these key areas as follows:

1. Data governance, which includes an overview of developments in the regulation of data protection and privacy in the country. This sub-section also highlights challenges and recommendations for the government’s consideration.

2. Cyber security, which focuses on the regulation of online security in the digital economy. This sub-section also highlights challenges and recommendations for the government’s consideration.

3. Encryption and surveillance, which focuses on the steps taken by the government to secure encryption and regulate electronic surveillance. This sub-section also highlights challenges and recommendations for the government’s consideration.

4. Cloud computing, which focuses on the development of cloud services in the country. This sub-section also highlights challenges and recommendations for the government’s consideration.

5. Emerging technologies, which focuses on the development of artificial intelligence and the internet of things. This sub-section also highlights challenges and recommendations for the government’s consideration.

6. Digital payments, which focuses on the regulatory framework that oversees digital transactions, with a focus on abating systemic risks. This sub-section also highlights challenges and recommendations for the government’s consideration.

7. Platform regulation, which focuses on the regulation of intermediaries and online content. This sub-section also highlights challenges and recommendations for the government’s consideration.

8. Competition law and digital taxation, which focuses on evolving issues in the areas of competition and digital taxation, insofar as they relate to the digital economy. This sub-section also highlights challenges and recommendations for the government’s consideration.
A. Context

As of June 2019, India does not have a specific legislation that regulates data protection. Currently, all categories of personal data do not have guaranteed protections against breaches of privacy, confidentiality and security under the Information Technology ("IT") Act. This is set to change with the enactment of the proposed Personal Data Protection Bill, 2018 ("PDP Bill"), which is due to be tabled in the Indian Parliament on a priority basis, as per the IT minister Shri. Ravi Shankar Prasad.

The constitution of the committee of experts under the chairmanship of Justice B.N. Srikrishna ("Srikrishna Committee") in July 2017 was a significant first step towards the creation of a comprehensive national data protection regime. This was followed by the Indian supreme court's recognition of the right to privacy as a fundamental right in the case of Puttaswamy v. Union of India. Within four months of the constitution of the Srikrishna Committee, it released a white paper seeking stakeholder comments on over 200 questions. Following a period of robust public stakeholder consultations, the Srikrishna Committee submitted its final report to the ministry of electronics and information technology ("MeitY") in July 2018. This report proposed recommendations for what a national data protection framework should look like. In keeping with the Srikrishna Committee's terms of reference the report also contained a draft personal data protection law, to which MeitY sought further feedback.

This draft personal data protection law must be tabled in the Indian parliament and approved before it can be enacted. In the meantime, different regulators have attempted to develop data protection and governance frameworks for their specific sectors. These developments have been discussed in detail below.

B. Current state of law and policy

Existing legal framework under the IT Act, 2000:

The IT Act is presently the only industry-agnostic law that protects the confidentiality, privacy and security of information across sectors.

The constitution of the committee of experts under the chairmanship of Justice B.N. Srikrishna ("Srikrishna Committee") in July 2017 was a significant first step towards the creation of a comprehensive national data protection regime. This was followed by the Indian supreme court's recognition of the right to privacy as a fundamental right in the case of Puttaswamy v. Union of India. Within four months of the constitution of the Srikrishna Committee, it released a white paper seeking stakeholder comments on over 200 questions. Following a period of robust public stakeholder consultations, the Srikrishna Committee submitted its final report to the ministry of electronics and information technology ("MeitY") in July 2018. This report proposed recommendations for what a national data protection framework should look like. In keeping with the Srikrishna Committee's terms of reference the report also contained a draft personal data protection law, to which MeitY sought further feedback.

This draft personal data protection law must be tabled in the Indian parliament and approved before it can be enacted. In the meantime, different regulators have attempted to develop data protection and governance frameworks for their specific sectors. These developments have been discussed in detail below.

Existing legal framework under the IT Act, 2000:

The IT Act is presently the only industry-agnostic law that protects the confidentiality, privacy and security of information across sectors.

---

Specifically, section 43A of the IT Act requires companies to implement reasonable security practices when dealing with sensitive personal data or information (such as passwords and financial information)\(^\text{113}\), failing which they can be required to pay damages to the affected persons\(^\text{114}\). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") notified under section 43A of the IT Act further regulate the collection, disclosure and transfer of sensitive personal data or information\(^\text{115}\). Section 72A of the IT Act protects the confidentiality of personal information by penalising the disclosure of such information, if the disclosure is non-consensual or in breach of a lawful contract\(^\text{116}\).

**The PDP Bill**

The data protection principles recommended by the report of the committee of experts on data protection ("Srikrishna Committee Report") are codified under the draft PDP Bill. This draft law creates a data governance framework that consists primarily of three players: (a) data fiduciaries (those who control the purpose and means of processing personal data, hereinafter referred to as "DFs")\(^\text{117}\); (b) data processors (those who process personal data on behalf of DFs, hereinafter referred to as "DPs")\(^\text{118}\); and (c) data principals (those whose personal data is processed by DFs or DPs)\(^\text{119}\). As the term suggests, DFs and data principals share a fiduciary relationship under the PDP Bill, meaning that the DF owes a duty of care to the data principal, and must act in their interests. This envisages a scenario where the rights of data principal must therefore be respected by law, and where the inequality in bargaining power between individuals and entities that process personal data is mitigated\(^\text{120}\). The PDP Bill contains a number of other checks and balances to ensure that the interests of data principals are protected. For instance, DFs are required to process the personal data of data principals in a fair and reasonable manner\(^\text{121}\), on the basis of legal grounds\(^\text{122}\), and only for purposes that are clear, specific and lawful\(^\text{123}\). Additionally, data principals are granted various rights, such as the right to be forgotten\(^\text{124}\), right to data portability\(^\text{125}\), the right to confirm whether DFs are processing/have processed their data, and to receive a brief summary of such personal data and the processing activities of such DFs\(^\text{126}\).

\(^{113}\) Rule 3, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: “Sensitive personal data or information of a person means such personal information which consists of information relating to:—(i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.”.

\(^{114}\) Section 43A, Information Technology Act, 2000.

\(^{115}\) The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.


\(^{117}\) Section 3(13), ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.

\(^{118}\) Section 3(15), ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.

\(^{119}\) Section 3(14), ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.


\(^{121}\) Section 4, ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.

\(^{122}\) Section 7, ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.

\(^{123}\) Section 5, ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.


\(^{125}\) Section 26(1)(a) & (b), ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_PROtection_Bill,2018.pdf.

The RBI's data localisation circular

In April 2018, the Reserve Bank of India (“RBI”) issued a notification mandating that all data related to payment systems be locally stored only in India. All payment system providers were required to comply with this notification within six months, i.e., by October 2018. In stark contrast to the Srikrishna Committee's relatively open and inclusive consultations, this was a unilateral decision taken by RBI. Several payment companies expressed concerns about the lack of transparency in RBI's decision-making process for this particular mandate and its refusal to extend the six-month deadline for compliance, without a publicly available cost-benefit analysis to justify the move. Such opaque decision-making processes run the danger of ignoring potential negative consequences on the country's economy.

Telecom Regulatory Authority of India’s privacy recommendations

Separately, in July 2018, the Telecom Regulatory Authority of India ("TRAI") released its own ‘Recommendations on privacy, data security, and data ownership in the telecom sector” ("TRAI Recommendations"). These recommendations were the product of a nearly year-long consultation process initiated by TRAI in August 2017. However, the TRAI recommendations differ from the Srikrishna Committee recommendations and the frameworks incorporated under the PDP Bill on several counts.

Draft E-Commerce Policy

The latest attempt at developing sector-specific data governance principles was made by the department for promotion of industry and internal trade ("DPIIT") under the ministry of commerce and industry, when it released a draft version of the National E-Commerce Policy ("Draft E-Commerce Policy"). As with the TRAI Recommendations, the Draft E-Commerce Policy’s recommendations on data governance also go over and above the standards prescribed under the PDP Bill. For instance, the Draft E-Commerce Policy specifies that any business entity that collects or processes sensitive data in India and stores it abroad must ensure that the data stored abroad is not shared with other business entities outside India, for any purpose, even with customer consent. It also provides that all such data stored abroad should not be made available to third parties, for any purpose, regardless of customer consent.

This recommendation overlooks the Srikrishna Committee’s views on the treatment of Sensitive Personal Data ("SPD") and cross-border flows of such data. The bar on the sharing of sensitive data, regardless of customer consent, ignores the Srikrishna Committee’s views on the importance of consent and contradicts the Draft E-Commerce Policy’s own stance that data is owned by individuals alone and requires their express consent for it to be shared. Additionally, the policy’s recommendation of a three-year time-frame for transitioning to storage in India appears to be short-sighted and requires reconsideration.

C. RECOMMENDATIONS

1. Harmonise the data governance frameworks under different instruments

The regulatory instruments on data governance adopted and proposed by the government have differing stances on a number of critical issues, which may lead to regulatory uncertainty. For instance, the Draft E-Commerce Policy differs from the PDP Bill on several important aspects, such as consent, categorisation of personal data, the relationships between data principals and DFs, the meaning of 'community data', and cross-border flows of data. Similarly, the RBI data localisation mandate differs from the PDP Bill on its approach towards data transfers. These inconsistencies will create uncertainty in the law, which in turn will affect the ease of doing business in India and stifle economic growth in the country. Therefore, it is recommended that all government policies on data governance should be harmonised in keeping with the frameworks suggested by the Srikrishna Committee and the PDP Bill, as these will serve as the basis for the national law on data protection.

2. Reconsider the imposition of data localisation

All the legislative and policy developments on data governance in the country thus far have advocated data localisation, i.e., the storage of personal data on servers located in India. However, there are a number of concerns with operationalising data localisation. First, the storage of all the country's critical data within India runs the risk of creating a "honeypot" of such data, which is vulnerable to cyber-attacks, foreign surveillance and other threats.

---

139 The Draft E-Commerce Policy, 2019, dated 23 February 2019 stresses that an individual's data can only be used with their express consent. This observation contradicts the data governance framework under the Personal Data Protection Bill, 2018 on two counts. First, it uses the term 'data' without explaining whether an individual's data represents their personal data or their sensitive Personal data, both of which require different standards of consent for processing under the Personal Data Protection Bill, 2018. Second, it squarely contradicts the Personal Data Protection Bill, 2018 which makes it clear that express consent is only required for the processing of sensitive personal data, and not personal data.
139 As explained above, the Draft E-Commerce Policy, 2019, dated 23 February 2019, uses the term 'data' without explaining whether an individual's data represents their personal data or their sensitive personal data.
140 The Draft E-Commerce Policy, 2019, dated 23 February 2019, states that the government is the gatekeeper of citizens' data, since it holds their data in trust. This approach is completely inconsistent with the frameworks laid down under Personal Data Protection Bill, 2018, which creates a fiduciary relationship between data fiduciaries and data principals.
141 The Draft E-Commerce Policy, 2019, dated 23 February 2019, recommends the creation of frameworks for sharing 'community data', a term which is left undefined. No such term has been referred to under the Personal Data Protection Bill, 2018, creating uncertainty as regards the meaning of 'community data' and the interaction of data sharing frameworks for such data under the Draft E-Commerce Policy, 2019 with the data governance frameworks under the Personal Data Protection Bill, 2018.
142 The recommendations of the committee of experts on a data protection framework for India, dated 23 February 2019 on cross-border data flows go over and above the standards prescribed under the Personal Data Protection Bill, 2018, without the backing of an accompanying law.
143 While the Reserve Bank of India data localisation mandate requires all data relating to payment systems in India to be stored only in India, the Personal Data Protection Bill, 2018 allows for the transfer of personal data and sensitive personal data under certain conditions.
Second, data localisation may have potentially harmful consequences for the Indian economy\textsuperscript{146}. For instance, a study by the Leviathan Security Group has found that for many countries that are considering or have considered mandatory data localisation laws, local companies would be required to pay 30-60 per cent more for their computing needsthan if they could go outside the country's borders\textsuperscript{149}. The European Centre for International Political Economy ("ECIPE") has also found that economy-wide data localisation laws drain between 0.7 per cent and 1.1 per cent of GDP from the economy for no benefit, since "any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy"\textsuperscript{150}.

Given the harmful consequences associated with mandatory data localisation, it is recommended that the government should reconsider the imposition of 'hard' data localisation. Alternatively, an incentive framework should be created to incentivise a voluntary shift to storage on local data servers in India in the long term, without disrupting ease of doing business in the country.

3. Reimagine consent for the digital age

Consent is one of the six legal grounds on the basis of which DFs can process personal data under the PDP Bill\textsuperscript{151}. This consent must be secured through a detailed notice that is provided no later than at the time of collection of personal data\textsuperscript{152}. Requiring DFs to provide extremely detailed notices at the time of collection of personal data creates a number of problems. For instance, it can lead to consent fatigue\textsuperscript{153} in cases where data collection takes place at multiple points over the same transaction, since notices will have to be provided each time the data is collected. This will undermine the data principal's ability to give meaningful and informed consent, since the amount of information provided with each notice is extensive. Given the vast amounts of personal data that is processed every day for each data principal, it is arguable that seeking a data principal's consent is no longer the best way to safeguard their privacy interests\textsuperscript{154}. The multiplicity of notices required under the PDP Bill may also stifle entrepreneurship in the country since many boot-strapped start-ups will lack the financial wherewithal to operationalise this requirement.

In order to tackle these concerns, it is suggested that an accountability-based model, where a higher degree of responsibility may be assigned to DFs, be considered for securing the interests of data principals. For instance, DFs must be responsible for the personal data that they collect and process. Further, the burden of evaluating the privacy risk that arises from the processing of a data principal's personal data must fall on the DFs, instead of on the data principals, and remedies should be offered to principals for privacy harms suffered, regardless of whether they were notified and gave consent\textsuperscript{155}.

4. Encourage cross-border flows

The PDP Bill, the RBI data localisation mandate and the Draft E-Commerce Policy, 2019 all place a number of restrictions on cross-border data flows that will lead to loss of market access and the latest technology by businesses in India, particularly startups\textsuperscript{156}. Such fetters may also reduce access to global cloud service platforms, application programming interfaces and analytical tools that are available in other jurisdictions\textsuperscript{157}.


\textsuperscript{149} Leviathan Security Group, Quantifying the cost of forced localisation, available at https://static1.squarespace.com/static/556340ece4b0b869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localisation.pdf.

\textsuperscript{150} The European Centre for International Political Economy, The costs of data localisation: A friendly fire on economic recovery, available at https://ecipe.org/publications/dataloc/.

\textsuperscript{151} Section 12, ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

\textsuperscript{152} Section 8(1), ministry of electronics and information technology, the Personal Data Protection Bill, 2018 (Note: data fiduciaries can provide data principals with a notice as soon as is reasonably practicable, if the data is not collected from the data principal.), available at https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.


\textsuperscript{154} R. Matthan, Consent is dead, available at https://www.livemint.com/Opinion/621SQ382WPGJKKBOHQRwHK/Consent-is-dead.html.


This may affect the competitiveness of Indian startups by reducing their ability to innovate, work efficiently and balance operational costs against their earnings. Restricting cross-border flows of data may even reduce access to global technological developments, such as developments relating to blockchain or artificial intelligence. In fact, the NITI Aayog in its National Strategy for Artificial Intelligence ("AI Strategy") noted that there is a shortage of "AI expertise, manpower and skilling opportunities in India"158. Thus, there is a need to focus on increasing expertise in AI and its adoption in India. The PDP Bill may adversely affect the goals of the AI Strategy if businesses are prevented from using AI based technology available outside India due to restrictions on cross border data flow.

Instead of restricting cross-border flows of data, inter-governmental measures that are based on a common set of norms (such as mutual recognition of domestic privacy laws, law enforcement co-operations and accountability) may be adopted to enable cross border data flows in India. The Asia Pacific Economic Co-operation ("APEC") Cross-Border Privacy Rules159 are an example of one such inter-governmental measure that may be adopted. The government should also consider the creation of a 'privacy shield' framework, along the lines of the EU-US and Swiss-US frameworks160, to encourage the smooth transfer of data between foreign and Indian companies. Further, the government should back the use of standard contractual clauses to facilitate cross-border flows of data. In order to facilitate cross-border transfers of data, the government can explore multilateral and bilateral avenues of effective co-operation between different countries. Further, existing instruments such as Mutual Legal Assistance Treaties ("MLAT")161 should be strengthened as well.

5. Remove criminal penalties

Offences under the PDP Bill are punishable with criminal penalties that include imprisonment sentences of up to 5 years162. Such penalties are excessively harsh and disproportionate, particularly since the civil penalties themselves function as effective deterrents against data breaches and other violations of the PDP Bill. Further, criminal penalties would disincentivise small and medium sized enterprises from participating in the digital economy. Therefore, it is recommended that the criminal penalties be removed from the PDP Bill.

6. The definition of the term ‘child’ under the PDP Bill should be amended

The PDP Bill defines a ‘child’ to mean a data principal below the age of 18 years163. In order to process a child’s data, data fiduciaries must incorporate appropriate mechanisms to verify their age and obtain parental consent164. It will be challenging for data fiduciaries to implement this requirement over the internet, as users are invisible online, making it difficult to ascertain whether a user qualifies as a child under the PDP Bill or not. For instance, in order to ascertain the age of users, data fiduciaries may require them to share official identification documents. Where such users are children, the processing of identification documents itself may result in a violation of the PDP Bill. Given these difficulties, it is recommended that the definition of “child” should be amended such that the parental consent requirements for children are in keeping with equivalent laws such as the European Union’s General Data Protection Regulation (“GDPR”)165, where parental consent is only required for children below the age of 16 years.

---

159 Asia Pacific Economic Cooperation, APEC Cross-Border Privacy Rules system program requirements, available at http://cbprs.org/business/.
7. **Revise the classification of data under the PDP Bill**

Indirectly identifiable data should be excluded from the ambit of ‘personal data’ under the PDP Bill. This is because, in order for a data fiduciary to ascertain whether data may indirectly identify a data principal, the data fiduciary will need to employ constantly evolving technological means, which will involve high compliance costs. Moreover, ‘indirectly identifiable data’ may also be read to include pseudonymised data, which will then qualify as personal data. This is problematic because data fiduciaries invest in pseudonymising data to use it for research and development purposes, which may not be possible if it is subject to the same safeguards as personal data.

8. **Remove financial data from the ambit of SPD**

The current definition of SPD may include all forms of financial data. Pure play financial identifiers (such as bank numbers or UPI handles) should be excluded from the ambit of SPD, since they cannot be abused to the detriment of the data principal. On the contrary, only data related to second factor authentication may be made SPD. This would be in line with the GDPR which also does not include financial data within the ambit of SPD.

---

166 Section 3(29), ministry of electronics and information technology, the Personal Data Protection Bill, 2018 available at https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill2018.pdf.
A. **Context**

As of June 2019, India does not have a comprehensive, cross-sectoral and dedicated law on cyber security. However, the IT Act and the rules framed under it do contain some provisions on these issues. These provisions have been discussed below.

Cyber security, electronic surveillance and encryption are closely interlinked, in that encryption is a means to maintain security and privacy of online communication, while law enforcement agencies that seek access to information by decryption or interception of encrypted communication are a means of state surveillance. In dealing with encryption and encrypted communications, the government has often preferred to forgo strong encryption for easier surveillance, which often compromises cyber security. Given this strong interconnection, this sub-section of the report can be read together with the following sub-section (Sub-section IV), which tackles electronic surveillance and encryption.

B. **CURRENT STATE OF LAW AND POLICY**

**Cyber security**

The IT Act defines ‘cyber security’ to mean the protection of a computer resource, communication device or information stored in it from "unauthorized access, use, disclosure, disruption, modification or destruction". In order to enhance cyber security measures, it empowers the central government to monitor and collect traffic data transmitted or stored in any computer resource.

**Protecting ‘critical information infrastructure’**

The IT Act defines ‘critical information infrastructure’ ("CII") to mean any computer resource the "destruction or incapacitation of which will have a debilitating impact on national security, economy, public health or safety". The central government is empowered to form a nodal agency to recognise and protect CII. This agency is known as the National Critical Information Infrastructure Protection Centre ("NCIIPC"). The NCIIPC’s function is limited to identifying and protecting CII.

---

167 The Information Technology Act, 2000.
168 Section 2(1) (nb), Information Technology Act, 2000.
169 Explanation (ii), section 69(B)(4), Information Technology Act, 2000: “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.
170 Section 2(k), Information Technology Act, 2000: “computer resource” means computer, computer system, computer network, data, computer data base or software.
171 Explanation to Section 70(1), Information Technology Act, 2000.
172 Section 70A, Information Technology Act: “The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection”.
CII notified as ‘protected system’

Both central and state governments are allowed to notify any computer resource which contains CII as a ‘protected system’. Once an organisation has been notified to have a ‘protected system’ it must observe certain security practices to secure the ‘protected system’ against unauthorised access, system vulnerabilities, cyber threats, etc. These organisations must also implement the security measures specified by NCIPC.179

Mechanism for responding to cyber security incidences

The government-appointed Indian Computer Emergency Response Team (“CERT-In”) is responsible for forecast, alerts and emergency response to cyber security incidents.179 It is allowed to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource for the purpose of enhancing cyber security.180

National Cyber Security Policy 2013

The National Cyber Security Policy181 was released by MeitY in 2013. However, as of June 2019, it has not been revised or updated. The policy captured the government’s principled intention to create a secure computing environment, build capabilities to prevent cyber-attacks and reduce cyber vulnerabilities.182

C. RECOMMENDATIONS

1. Formulate implementation strategies for the National Cyber Security Policy 2013

The National Cyber Security Policy 2013 identifies key principles and goals to strengthen the cyber security framework in India. However, it does not clearly articulate implementation strategies or a time frame to operationalise these goals. As a result, several principles envisaged in the policy have not effected regulatory change, despite there being an intent to do so. Therefore, the goals and principles given in the National Cyber Security Policy 2013 must be operationalised to effect policy change.

---

175 Section 2(e), Information Technology Act, 2000: “appropriate government” means as respects any matter: (i) enumerated in List II of the Seventh Schedule to the Constitution; (ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government.”

176 Rule 2(1)(k), Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018: “any computer, computer system or computer network of any organisation as notified under section 70 of the Act, in the official gazette by appropriate Government.”


179 Section 70B (4), Information Technology Act, 2000: “The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:– (a) collection, analysis and dissemination of information on cyber incidents; (b) forecast and alerts of cyber security incidents; (c) emergency measures for handling cyber security incidents; (d) coordination of cyber incidents response activities...”.

180 Rule 2(h), Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 states “Cyber Security Incident” means any real or suspected adverse event that is likely to cause or causes and offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorization; or threatens public safety, undermines public confidence, have a negative effect on the national economy or diminishes the security posture of the nation.”


2. **Encourage private sector participation in policy formulation**

The regulatory framework governing cyber security in India has largely been formulated by the government, without private sector participation. This approach is out of alignment with the National Cyber Security Policy 2013, which aims to develop an "effective public private partnership and [create] models for collaboration and engagement of various stakeholders including private stakeholders". Given the dynamic nature of cyber threats which create new vulnerabilities and opportunities for disruption from a variety of sources, the lack of private sector participation in formulating policies thwarts adoption of innovative and nimble solutions to combat cyber threats. Therefore, formulating policies effecting cyber security should have more private sector participation. This would enable the creation of a robust and future-ready regulatory framework, which is able to counter and minimise cyber security threats.

3. **Strengthen regulatory accountability**

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 do not hold the CERT-In accountable for its treatment and quality of response to cyber security incidents. This level of discretion granted to the CERT-In creates a lack of regulatory accountability. This can be remedied by amending the CERT-In Rules to mandate the minimum response time and standard response procedure that the CERT-In must follow in its response to cyber security incidences. Further, law enforcement access requests by government agencies should aim to be lawful, fair, specific and limited such that the personal data being requested is not excessive. The government can also limit the discretion granted to intelligence agencies for accessing personal data by permitting such access requests only if they are required for a specific purpose under a statutory authority, as is practiced in the UK.

4. **Arrest the rise in cyber-security breaches**

There have been reports of up to 6,50,000 cyber-attacks on the Indian government's systems from countries like China, Russia and the US. This clearly demonstrates that the cyber security protocols are currently lacking on the implementation and policy fronts. It indicates the need for an improved regulatory mechanism to secure the data of the government, Indian citizens and businesses. Therefore, a robust and comprehensive cyber security law is needed to protect the vast data reserves in India's rapidly growing digital economy.

5. **Reconsider data localisation**

As mentioned under the sub-section on data governance, the data localisation requirement under the PDP Bill will make the data of Indian citizens more vulnerable to security risks. This is because storing data across several jurisdictions increases the level of security and helps in data recovery in case of any disasters. The requirement to store at least one copy of ‘personal data’ within servers in India may lead to duplicate sets of data being stored in multiple servers within and outside India. This will increase the number of attack surfaces for the same sets of data thereby exacerbating the possibility of data breach. Therefore, the data localisation framework must consider unintended consequences such as the exacerbation of cyber security threats. Our recommendations on this issue have been captured in the sub-section on data governance.
6. Promote more resilient authentication processes

The government may consider promoting risk based authentication ("RBA") or multi-factor authentication ("MFA") over two-factor authentication ("2FA"). Currently, most device and resource-security measures follow a 2FA process where a possession factor (such as possession of a mobile device to receive a one-time-password) is added to a knowledge factor (such as knowing the password to access a mail account). Unwittingly, the possession factor used by most players is a one-time-password, which may create complications in remote areas where signal connectivity is weak. Additionally, 2FA is not immune to breach. These concerns can be addressed by resorting to MFA or RBA. MFA may include factors like biometrics, smart cards, security tokens over and above the possession and knowledge factors. RBA involves an assessment of the login device, IP reputation, geolocation and geovelocity of each login (some or all may be assessed) and churns out risk scores for every login. Additional factors of authentication are solicited if the risk score is deemed to be high. RBA is thus more flexible, contextualised and robust compared to 2FA or MFA. These measures will contribute to enhancing transactional security (security of communications between multiple entities to complete an online transaction, such as an e-commerce purchase) as well.

---

191 Kaspersky Daily, SMS-based two-factor authentication is not safe — consider these alternative 2FA methods instead, available at https://www.kaspersky.co.in/blog/2fa-practical-guide/14467/.

192 Kaspersky Daily, SMS-based two-factor authentication is not safe — consider these alternative 2FA methods instead, available at https://www.kaspersky.co.in/blog/2fa-practical-guide/14467/.


A. Context

India does not have a comprehensive law on encryption or surveillance. Various legislations and sectoral guidelines prescribe standards for the encryption, and conditions for the interception of communications and the decryption of data. Encryption, decryption and surveillance are broadly interconnected subjects. Therefore, they are governed by overlapping instruments and judgments.

Under current law, encryption is "the process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption)". The decryption process requires a key; the longer the key, the more security it offers. Law enforcement agencies argue for easier decryption or access to the decryption key altogether. On the contrary, users want greater security and privacy of their communications and prefer stronger encryption.

The Information Technology Act, 2000 ("IT Act"), the various rules framed under it, the Indian Telegraph Act, 1885 ("Telegraph Act"), and the Indian Telegraph Rules, 1951 ("Telegraph Rules") govern the encryption and the interception of information. The Telecommunications Intermediaries (Intermediary guidelines (Amendment) Rules) 2018 ("Draft Intermediary Guidelines") make some proposals on interception and traceability. The draft Personal Data Protection Bill, 2018 ("PDP Bill") contains stipulations toward the encryption of sensitive personal data and information. The Unified Licence Agreement ("ULA") released by DoT also contains several clauses which speak to encryption and surveillance. The Telecom Regulatory Authority of India ("TRAI") released recommendations on privacy in 2018 which also briefly discuss cyber security, encryption and surveillance in India.

The Supreme Court, in the People’s Union for Civil Liberties v. Union of India ("PUCL Case"), laid down certain checks and balances on the government’s use of its powers of decryption and interception. In K.S. Puttaswamy v. Union of India (2017) ("Puttaswamy Case"), the Supreme Court declared privacy to be a fundamental right. It stated that this fundamental right could be restricted only if the ‘Three Part Test’ was satisfied.

Law enforcement agencies argue for easier decryption or access to the decryption key altogether. On the contrary, users want greater security and privacy of their communications and prefer stronger encryption.
In K.S. Puttaswamy v. Union of India (2018) (“Aadhaar Case”) the Supreme Court ruled that the Aadhaar system was constitutional because it satisfied the Three-Part Test and stated that the Aadhaar system did not tend to create a surveillance state in India.

B. CURRENT STATE OF LAW AND POLICY

IT Act

The central government is empowered to prescribe modes and methods of encryption under the IT Act. In 2015, the government published a draft encryption policy which was soon withdrawn due to sharp public criticism. The ministry of electronics and information technology (“MeitY”) was reportedly compiling a second version of the same in mid-2016, but this has not been released yet.

Information Technology (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009

The central government has the power to intercept, monitor and decrypt any communication generated, transmitted, received or stored in a computer resource through a written order (“Surveillance Order”) which may be given in the “interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence.” Accordingly, the Ministry of Home Affairs issued an order authorising ten “security and intelligence” agencies to issue Surveillance Orders (“MHA Order”). The central government also has the power to authorise any agency to collect and monitor any information which is generated or stored in any computer resource for ‘enhancing cyber security’ and/or for preventing the spread of a ‘computer contaminant’. While on one hand this provision seeks to enhance cyber security, on the other hand it may also compromise the privacy of common Indian citizens.

209 K.S. Puttaswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012.
215 Section 2(k) of the Information Technology Act defines ‘computer resource’ as any computer, computer system, computer network, data, computer databases or software. The terms ‘computer’, ‘computer network’ and ‘computer system’ are defined in sections 2(i), 2(j) and 2(l) of the Information Technology Act 2000.
217 Explanation (i), Section 43, Information Technology Act, 2000: “‘computer contaminant’ means any set of computer instructions that are designed-
(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system, or computer network.”
**Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011**

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") require certain entities to put in place an information security policy. Since these are aimed at protecting consumer data, companies are inclined to adopt high standards of encryption, which will in turn keep their data safe. The SPDI Rules state that these information security policies may either comply with industry best practice standards or an industry association may create its own code, which it must then get ratified by the central government.

**TRAI Recommendations**

TRAI recommended the harmonisation of the encryption standards across different sectors and the formulation of a national policy for the encryption of personal data. Further, it recommended that personal data of telecom consumers should be encrypted during motion and storage, and decryption should be permitted only after obtaining customer consent.

**Draft Intermediary Guidelines**

The Draft Intermediary Guidelines stipulate that an intermediary upon a request from a government agency should provide the requested information to the agency within 72 hours of receiving such order ("Access Order"). Further, the Draft Intermediary Guidelines propose that intermediaries should enable tracing of a message back to its originator, if required by certain authorised government agencies. These are both forms of monitoring and surveillance; if implemented in their current form the Draft Intermediary Guidelines would increase the surveillance capabilities of government manifold.

**PDP Bill**

The PDP Bill requires any legal or juristic person including the government (collectively "person") who collects and/or processes personal data of other people to implement safeguards, including encryption, to protect such data.

---

220 Rule 8, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
221 Rule 8(2), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
222 Rule 8(3), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
226 TRAI Recommendations
227 Draft Intermediary Guidelines
228 PDP Bill
The PDP Bill also proposes to establish a Data Protection Authority ("DPA") which has the power to inquire into the affairs of any person which collects and/or processes the personal data of people. If any such person fails to assist the DPA, it may "access any computer, computer resource, or any other device containing or suspected to be containing data." Under the PDP Bill, sensitive personal data also includes passwords. If passwords include decryption keys, then the PDP Bill restricts the storage of such decryption keys outside India.

**Telegraph Act and Telegraph Rules:**

Central and state government officials can temporarily take control of any licensed telegraph (as defined under the Telegraph Act) without any written order. They may stop the transmission of certain messages, or demand their disclosure. Certain government officials may pass orders for the interception of information ("Interception Orders") which establish a review committee to review Surveillance Orders and Interception Orders. This means that government officials review orders passed by other government officials without any legislative or judicial oversight. In the PUCL Case, the Supreme Court laid out that Interception Orders should be issued only by the state or central home secretaries, that the agency making such an order should consider whether there are other means to access such information other than interception, that the Interception Order should be specific and detailed, and lastly that the Interception Order should be valid only for two months.

**ULA**

The ULA prohibits the use of bulk encryption (bulk encryption is a process used for encrypting large amounts of data) and stipulates that the "use of encryption by the subscriber shall be governed by the Government Policy/rules made under the Information Technology Act, 2000." Therefore, the ULA does not prescribe any

---

232 Section 49 of the Personal Data Protection Bill sets up the Data Protection Act. Section 60 of the Personal Data Protection Bill lays down the various powers and functions of the DPA, which include primarily, the protection of the interests of data principals, ensuring compliance with the provisions of the PDP Bill and promoting awareness of data protection, available at [https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf](https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf).

233 Section 64(1), Ministry of electronics and information technology, the Personal Data Protection Bill 2018, available at [https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf](https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf).

234 Sections 66(1) (iii), and 66(11) (b), Ministry of electronics and information technology, the Personal Data Protection Bill 2018, available at [https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf](https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf).

235 Section 3(35), Ministry of electronics and information technology, the Personal Data Protection Bill 2018, available at [https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf](https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018%2C0.pdf).


237 Section 3, (1AA), Telegraph Act, 1885: "telegraph" means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means. Explanation. —"Radio waves' or 'Hertzian waves' means electromagnetic waves of frequencies lower than 3,000 giga-cycles per second propagated in space without artificial guide."

238 Section 5(1), Telegraph Act.

239 Section 5(2), Telegraph Act.

240 Rule 419A, Telegraph Rules.


242 Rule 419A, Telegraph Rules.


244 Para 35(1), People’s Union for Civil Liberties v. Union of India, Writ Petition (Criminal) No. 612 of 1992.


249 Definition of Terms and expressions, Department of telecommunications, Licence Agreement for Unified Licence: "90. SUBSCRIBER means any person or legal entity, which subscribes to / avails of the service from the Licensee. In this License, the words ‘Customer’ and ‘Subscriber’ have been used interchangeably.”

Various encryption guidelines

Various sectoral regulators have formulated sector-specific encryption guidelines. For example, the Securities Exchange Board of India (“SEBI”)\(^253\), the Reserve Bank of India (“RBI”)\(^254\) also lay out guidelines for the sectors they oversee.

Puttaswamy Case

The Supreme Court held that the right to privacy was a fundamental right\(^255\). It laid down the Three-Part Test to determine whether any restriction on the right to privacy was legal. These three conditions are that

(i) the restriction must be based on an existing law, i.e. should be lawful in nature (‘legality’); (ii) the restriction should achieve a legitimate state aim (‘legitimate purpose’); (iii) the extent of restriction must be proportionate to achieve the legitimate aim (‘proportionality’).\(^256\) The Supreme Court directed the government to introduce a strong data protection regime in India as soon as possible. The draft PDP Bill submitted to MeitY is a step in this direction\(^257\).

Aadhaar case

The Supreme Court ruled that the Aadhaar system was constitutional\(^258\) since it satisfied the Three-Part Test and stated that the Aadhaar system did not tend to create a surveillance state in India\(^259\).

---

258 Para 1173, K.S. Puttaswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012.
C. RECOMMENDATIONS

1. Align the various laws governing cyber security, encryption and surveillance

SEBI\textsuperscript{260} and RBI\textsuperscript{261} prescribe different encryption standards while the ULA does not prescribe any\textsuperscript{262}. Moreover, the IT Act, Telegraph Act, and the rules framed under them, as well as the PDP Bill, Draft Intermediary Guidelines, and ULA all have overlapping and conflicting provisions concerning encryption, surveillance and interception. The government should create an overarching regime for cyber security, encryption and surveillance which balances individual privacy and business interests in keeping information secure with the law enforcement objectives.

2. Adopt leading industry standards for encryption

Many instruments today stipulate very low standards of encryption, such as 128-bit encryption, which is easy to decrypt\textsuperscript{263}. Very low standards of encryption may leave businesses and government datasets vulnerable to backdoor or zero-day attacks by the enemies of the state. Therefore, the government should encourage the adoption of leading industry standards for encryption.

3. Prescribe narrow grounds for decryption

The Telegraph Act, the PDP Bill and the IT Act have broad grounds for issuing interception and Surveillance Orders. Terms such as ‘to enhance cyber security’\textsuperscript{264}, ‘interest of public safety’\textsuperscript{265}, and ‘detrimental to interests of data principals’\textsuperscript{266} under the IT Act, Telegraph Act and PDP Bill respectively, are broad. It is unclear whether decryption keys fall under the definition of passwords under the PDP Bill or not. These grounds should be brought in line with the Puttaswamy Case.

4. Introduce legislative or judicial oversight over government surveillance:

Under current Indian law, the executive pillar of the country sits in review over orders passed by the executive\textsuperscript{267}. This may compromise neutral and unbiased decision making and also goes against the basic principle of law that a person must not judge his own case\textsuperscript{268}. The government should introduce some legislative or judicial oversight into this process to strengthen it. This is the case in several countries such as the US, UK, South Africa and Germany\textsuperscript{269}.

---


\textsuperscript{261} Reserve Bank of India, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, dated 29 April 2011, available at https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf. These guidelines mandate the use of at least 128-bit encryption and other cyber security related measures which banks may take.

\textsuperscript{262} SFLC, FAQ: Legal Position of Encryption in India, available at https://sflc.in/faq-legal-position-encryption-india.


\textsuperscript{264} Section 69B, Information Technology Act.

\textsuperscript{265} Sections 5(1) and 5(2), Telegraph Act.

\textsuperscript{266} Section 64, Ministry of electronics and information technology, the Personal Data Protection Bill 2018, available at https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

\textsuperscript{267} N. Chaudhari and T. Joshi, Centre’s order on computer surveillance is backed by law – but the law lacks adequate safeguards, available at https://scroll.in/article/906764/centres-order-on-computer-surveillance-is-backed-by-law-but-the-law-lacks-adequate-safeguards.

\textsuperscript{268} N. Chaudhari and T. Joshi, Centre’s order on computer surveillance is backed by law – but the law lacks adequate safeguards, available at https://scroll.in/article/906764/centres-order-on-computer-surveillance-is-backed-by-law-but-the-law-lacks-adequate-safeguards.

\textsuperscript{269} N. Chaudhari and T. Joshi, Centre’s order on computer surveillance is backed by law – but the law lacks adequate safeguards, available at https://scroll.in/article/906764/centres-order-on-computer-surveillance-is-backed-by-law-but-the-law-lacks-adequate-safeguards.
5. **Disclose requisitions to impacted persons:**

The government should mandate that requisitions of information about a particular person should be communicated to him/her and should even specify the timelines for such disclosure. This would enhance transparency in the exercise of the government’s powers.

6. **Retain end to end encryption**

The government’s proposal to enable traceability under the Draft Intermediary Guidelines will detrimentally impact the right to free speech and privacy. Both of these are cherished constitutional values and must be upheld. Therefore, end to end encryption should be retained. Moreover, end to end encryption is broken through the use of encryption backdoors. Knowledge of such backdoors to encrypted platforms will prompt zero-day attackers and hackers and to find ways to exploit this backdoor to gain access to sensitive data.

7. **Allow bulk encryption:**

Bulk encryption provides a high degree of security. A ban on bulk encryption as prescribed by the ULA decreases cyber security in India and increases business costs. The ban of bulk encryption should be lifted to facilitate better information security, and reduce compliance costs.

---


REGULATION OF CLOUD SERVICE PROVIDERS

A. Context

Cloud computing services are transforming the manner in which Information Technology ("IT") services are consumed and managed, resulting in improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. The government has also recognised these advantages and has sought to integrate cloud computing technology for the delivery of e-services in India. It is also proactively looking to establish India as a global hub for cloud computing and to facilitate the growth of cloud service providers ("CSP")275. However, certain proposals of the central government, especially pertaining to sector specific frameworks for CSPs276, will detrimentally impact cloud computing in India.

TCSPs provide information technology related services and therefore have largely been regulated by the ministry of electronics and information technology ("MeitY"). However, CSPs use telecom infrastructure to provide their services which is governed by the Indian Telegraph Act, 1885 ("Telegraph Act")277 and the Indian Telegraph Rules, 1951 ("Telegraph Rules")278. Since the Telegraph Act and the Telegraph Rules are administered by the ministry of communications and the department of telecommunications ("DoT"), there has been a regulatory overlap between the ministry of communications and MeitY in matters pertaining to CSPs. The Telecom Regulatory Authority of India ("TRAI") released recommendations on CSPs279 which exemplifies this overlap.

The IT Act governs the following issues for CSPs:
(i) data protection standards and practices280; (ii) co-operation with government authorities281; (iii) due diligence standards282; (iv) encryption standards283; (v) reporting obligations284; (vi) safeguards to protect against cyber-terrorism285; (vii) electronic service delivery of public services286; (viii) management of critical information infrastructure287.

B. Current state of law and policy

The IT Act governs the following issues for CSPs:
(i) data protection standards and practices; (ii) co-operation with government authorities; (iii) due diligence standards; (iv) encryption standards; (v) reporting obligations; (vi) safeguards to protect against cyber-terrorism; (vii) electronic service delivery of public services; (viii) management of critical information infrastructure.

---

277 The Indian Telegraph Act, 1885.
278 The Indian Telegraph Rules, 1951.
285 Engaging in cyber-terrorism is punishable with imprisonment under Section 66F of the Information Technology Act, 2000.
286 The Information Technology (Electronic Service Delivery) Rules, 2011.
287 The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.
Each of these issues is regulated by a comprehensive set of rules notified under the IT Act. CSPs are service providers under the Consumer Protection Act, 1986 ("COPRA") and are required to ensure that the quality, nature and manner of performance of their services abide by the standards set out under the IT Act and the rules framed thereunder and other commercial terms. Failure to abide by these requirements may invite action under the COPRA. The Reserve Bank of India's ("RBI") notification on cyber-security frameworks for banks also touches upon the use of cloud services by banks. The Insurance and Regulatory Development Authority of India's ("IRDAI") guidelines on information and cyber security of insurers provide guidance on cloud access control and cloud data security to ensure that information processed, transmitted and stored by CSPs is secure.

The MeghRaj framework prescribes standards for security, interoperability, and data portability, amongst others, which CSPs must comply with to become government empanelled CSPs. If implemented in its current form, the Draft E-Commerce Policy, the PDP Bill and the Draft Information Technology (Intermediaries Guidelines (Amendment) Rules) 2018 will also affect the data protection, privacy and due diligence standards applicable to CSPs. The Gopalakrishnan Committee's draft report reportedly stated that data generated in India should be stored locally for ease of access during investigations. Gopalakrishnan stated that a "forward looking" data protection regime was needed as India's information technology laws framework was "not sufficient" for cloud computing.

---


289 Section 2(o), Consumer Protection Act, 1986: "service" means service of any description which is made available to potential users and includes, but is not limited to, the provision of facilities in connection with banking, financing insurance, transport, processing, supply of electrical or other energy, board or lodging or both, housing construction, entertainment, amusement or the purveying of news or other information, but does not include the rendering of any service free of charge or under a contract of personal service.

290 Sections 2(1)(c)(ii), 2(1)(g), 11, 17 and 21, Consumer Protection Act, 1986.


298 In 2012, the then minister for telecom and information technology, Shri Kapil Sibal set up a committee under the chairmanship of Infosys's co-founder, Shri S. Gopalakrishnan to recommend a framework for cloud computing. See Press Trust of India, Kris Gopalakrishnan to head govt cloud computing panel, available at https://www.thhindubusinessline.com/info-tech/kris-gopalakrishnan-to-head-govt-cloud-computing-panel/article20468190.ece.


C. RECOMMENDATIONS

1. **Allow cross border flow of data**

The PDP Bill, Draft E-Commerce Policy and an RBI notification restrict cross border flows of data. CSPs prefer to locate their data centres in jurisdictions with cheap real estate, uninterrupted supply of electricity and water, cheap air conditioning infrastructure and lower temperatures as it is more cost efficient. Shifting their data centres to India may prove costly for most CSPs. Moreover, India’s geography is susceptible to earthquakes, floods, landslides and avalanches. Therefore, free flows of data across jurisdictions should be allowed to keep CSPs viable and to increase the range of service they offer to Indian consumers. This will also enhance innovation and entrepreneurship in the country on account of access to low-cost cloud storage and computing services which will help achieve the goals of the ‘Digital India’ programme.

2. **Ease regulatory burden on CSPs**

The government claims to believe in light touch regulation for CSPs. However, there are several proposals pertaining to the registration of CSPs, and the requirement for CSPs above a certain threshold value to become a member of such industry bodies. The government should ease the regulatory burden on CSPs and implement a light tough regulation in the true spirit of the word.

3. **Govern CSPs under the ambit of the MeitY**

The recommendations made by TRAI indicate a conflict between the ministry of communications and the MeitY. CSPs should remain under the ambit of MeitY since they provide information technology related services. The present regulatory framework has so far proven to be conducive to the growth of cloud computing services. It is recommended that any improvements in regulatory regimes be implemented by amending the current legal framework as required, rather than supplanting it with an entirely new piece of legislation.

4. **Allow CSPs to build and light their own fibre**

As a means to establish India as a hub for global cloud computing, the NDCP recommends that CSPs should be allowed to establish captive fibre networks. Implementing this recommendation is a step in the right direction and will enable CSPs to improve their service offerings in India, which in turn will benefit Indian consumers.

---

EMERGING TECHNOLOGIES: ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS

A. Context

As of June 2019, there are no distinct legislations, rules or regulations which govern artificial intelligence ("AI") and the internet of things ("IoT")/Machine-to-Machine learning ("M2Mlearning")\(^{312}\). There are multiple legal, regulatory and policy instruments issued by different government agencies which influence the regulation of these technologies. These include the Personal Data Protection Bill, 2018 ("PDP Bill") \(^{313}\), the Information Technology Act, 2000 ("IT Act")\(^{314}\), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules")\(^{315}\), and the Draft National E-commerce Policy ("Draft E-Commerce Policy")\(^{316}\).

Specific instruments which speak to IoT regulation in India are the National Telecom M2M Roadmap ("M2M Roadmap")\(^{317}\) and the IoT Policy document ("IoT Policy")\(^{318}\). Telecom Regulatory Authority of India's ("TRAI") consultation paper on spectrum, roaming and quality of service related requirements in M2M communications ("TRAI M2M Consultation Paper")\(^{319}\), its recommendations on spectrum, roaming and quality of service related requirements in M2M communications ("TRAI M2M Recommendations")\(^{320}\), and the Department of Telecommunications ("DoT") issued instructions for implementing restrictive features for SIMs used only for Machine-to-Machine communication services ("M2M SIM Guidelines")\(^{321}\).

There are multiple legal, regulatory and policy instruments issued by different government agencies which influence the regulation of these technologies.

Internet of Things

Presently, there are two dedicated resources on developing AI frameworks in India. These are the government-constituted task force report on AI for India’s Economic Transformation ("AI Task Force Report")\(^{322}\) and the NITI Aayog’s ‘National Strategy for Artificial Intelligence’ ("AI National Strategy")\(^{323}\).


\(^{314}\) The Information Technology Act, 2000.

\(^{315}\) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.


\(^{321}\) Department of telecommunications, Instructions for implementing restrictive features for SIMs used only for Machine-to-Machine (M2M) communication services (M2M SIMs) and related to Know Your Customer (KYC) instructions for issuing M2M SIMs to entity/organisation providing M2M Communication Services under bulk category and instructions for Embedded-SIMs (e-SIMs), dated 16 May 2018, available at http://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1.


B. CURRENT STATE OF LAW AND POLICY

Internet of Things

IoT service providers in India have to comply with the standards for handling personal data as per Section 43A of the IT Act and the SPDI Rules framed under it at present. Once the PDP Bill is enacted, these service providers will have to comply with its stipulations on notice, consent, purpose limitation, collection limitation, codes of practice, and cross-border transfer, amongst other things.

For all stakeholders who wish to participate in the M2M communications industry in India, the M2M Roadmap serves as the main point of reference at present. It recommends the registration of M2M service providers with the DoT and states that they should be governed by relevant DoT guidelines, in addition to the applicable laws of the land. The TRAI M2M Recommendations echo this recommendation as well. TRAI also recommends ‘graded’ security certifications for devices according to their functionality, the sensitivity of the data that they collect and the costs of remedying security lapses.
Artificial Intelligence

As of June 2019, there is no consolidated legal framework which regulates the functioning of AI in India. Until such time as this framework is developed, AI service providers will also have to comply with the provisions of the IT Act, SPDI Rules and the PDP Bill like IoT service providers, since they also collect personal and/or sensitive personal information from their customers. As regards policy-making for AI, the AI Task Force Report identifies standard setting for AI as an important goal in the AI space. This would include data storage and privacy standards, communication standards for autonomous systems and standards for interoperability between AI systems.335

The latest document which has shaped the way forward on policy making for AI is the NITI Aayog’s AI National Strategy. It identifies five priority sectors for focused intervention: healthcare336; agriculture337; education and skilling338; smart cities and infrastructure339; and smart mobility and transportation340. It also makes recommendations for increasing the uptake of AI in India. These include improving research capabilities, reskilling of labour, facilitating adoption of AI through democratisation of data and making it accessible to start-ups and researchers, and addressing concerns around ethics, privacy and security of AI.344

C. RECOMMENDATIONS

Internet of Things

1. Introduce relaxed standards of consent for IoT devices

IoT service providers will face a number of practical impediments in operationalising the current requirements for notice and consent under the PDP Bill.345 For instance, IoT devices that lack large display screens such as smartwatches and smart home appliances will simply be unable to display notices to customers. In other cases, seeking the consent of individuals for data collection can even defeat the purpose of IoT devices like security cameras. For technologies that use facial recognition to track management and attendance of a group, obtaining the consent of hundreds of individuals simultaneously will be impracticable. Therefore, some degree of flexibility in the standards of notice and consent imposed on IoT service providers would go a long way in ensuring that they can deliver their full range of benefits to consumers without being obstructed by onerous compliances. IoT developers and service providers may have to coordinate with the Data Protection Authority proposed to be established under the PDP Bill to develop practical guidelines to work around these issues.
2. **Revise purpose limitation requirements for IoT devices**

IoT service providers cannot always inform consumers of the purposes for which their personal data is being processed at the time of data collection, as is required under the PDP Bill. This is because it is difficult to limit the purpose for which personal data may be used in the future in the case of IoT ecosystems, as these purposes continue to evolve with the evolving functionality of IoT devices. For instance, a simple software update can transform the functionality of a smartphone such that it becomes capable of fulfilling new purposes with the personal data it collects. Thus, the purpose limitation requirements as prescribed under the PDP Bill must be revised such that they can be applied to IoT service providers.

3. **Introduce device-specific certification standards**

The IoT ecosystem offers immense possibilities in India for value addition in the lives of regular consumers, revenue generation and employment. However, the government must take measures to create a conducive market for IoT device and component manufacturers. A helpful step in this direction would be to act upon TRAI’s recommendation to provide differential certifications for different IoT products. The rationale for this is that products with different levels of functionality, security concerns and data collection capabilities should not be fettered by onerous certification requirements since this would impede manufacturing in the country. This will also allow devices such as IoT enabled smartphones to have different certification requirements compared to IoT enabled smart-bulbs, which have entirely different functionalities.

4. **Encourage adoption of IoT within the government**

Adequate capacity building interventions for government officials will ensure that they can leverage IoT as a tool to resolve their problems and resource constraints. A standardised module of training for government officials should be prepared and tested on a pilot basis and be rolled out on a large scale if it is successful.

5. **Promote consumer awareness**

It is important to instil confidence in IoT devices and their security to encourage the adoption of these devices in the Indian market. Therefore, the government should promote user education, including training on how to ensure the security of IoT devices through customisable passwords, biometric passwords and external software such as firmware. Consumers should also be made aware of the various benefits that IoT devices can bring to their lives in terms of convenience, energy conservation, and lower costs.

6. **Recognise global best practices for IoT devices**

Consumer confidence in IoT devices will be greatly improved with the recognition of global best practices, standards and certifications regarding the security and quality of IoT devices. This could be along the lines of the system followed by the “TÜViT” for information and communication technology in Germany. They assess security and quality characteristics against agreed and transparent standards and create the necessary trust in information technology products, systems and processes.
Artificial Intelligence

1. Develop an implementation roadmap

The AI National Strategy does not call for comments or responses from stakeholders, thereby providing little clarity on the next steps to be taken towards promoting AI in India. Therefore, the government should develop an implementation roadmap that tailors the broad-based recommendations of the AI National Strategy for different sectors to ensure their practical applicability.

2. Revise purpose limitation requirements for AI

Just as with IoT service providers, AI service providers will be unable to meet the purpose limitation requirements under the PDP Bill. Therefore, the revisions to the purpose limitation requirements for IoT service providers should be made applicable to AI service providers as well.

3. Discuss patents frameworks for AI algorithms

Presently, section 3(k) of the Patents Act, 1970 exempts AI algorithms from being patented. This severely deters AI development in the country and exposes AI developers to intellectual property theft. Thus, the government should seriously consider developing a patents framework for the protection of AI algorithms.

4. Address privacy concerns associated with AI

The AI National Strategy suggests the adoption of intelligent surveillance systems, including social media intelligence platforms to track people. This may conflict with existing privacy laws, the proposals of the PDP Bill, and individual privacy and freedoms including speech and assembly. All steps taken by the government towards the adoption and development of AI in the future must consider these inconsistencies and resolve them at the earliest.

5. Improve consumer awareness

As is the case with IoT, the AI ecosystem too must inspire the confidence of the Indian consumer base in terms of safety and privacy. This can be done by organising workshops and undertaking live demonstrations of different AI use cases. This recommendation finds place in the AI National Strategy as well. The government can also ensure that it increases the familiarity of citizens with AI by incorporating elements of AI in everyday public life. Such integration can take the form of AI use for traffic optimization, predictive maintenance of public infrastructure, and customer service activities.
6. **Introduce AI in government offices**

The uptake of AI technologies in society can also be catalysed by building capacity and trust in the government workforce. The government should encourage the adoption of AI applications in the workplace. This would ensure that there is a sense of ownership and accountability in the use of AI technology in government departments and instil a sense of trust and comfort within this technology. The absorption of AI technologies by government offices will lead to improved efficiency, quality and security of administrative services. A live use case is presented by the Department of Homeland Security in the US. The Department of Homeland Security’s Citizenship and Immigration and Services has created a virtual assistant, EMMA, that can respond accurately to human language. EMMA shows relevant answers to questions posed to it and answers almost half a million questions per month. EMMA learns from its own experience and gets smarter as it answers more questions.

Using AI in government offices would also help overcome resource constraints. This in turn would allow for resource redistribution and workforce optimization. For instance, a study reported that electronic document discovery, located 95 per cent of relevant documents for legal cases, compared to an average of 50 per cent for humans. Further, this exercise was completed by AI technology in a fraction of the time that humans needed. As a natural consequence, paperwork burdens would be reduced, which would automatically reduce backlogs.
DIGITAL PAYMENTS

A. Context

A digital payment is the transfer of funds which is initiated by a person by way of an instruction, authorisation or order to a bank to debit or credit an account maintained with that bank through electronic means. These payments are facilitated with the use of ‘payment systems’ which enable payments to be effected between a payer and a beneficiary, and include any system enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. In India, a ‘payment system’ can only be operated by entities authorised by the Reserve Bank of India (“RBI”). Apart from payment systems, various technology service providers, infrastructure providers and merchants also participate in the digital payments landscape by partnering with entities authorised and regulated by RBI.

B. Current state of law and policy

Licensing payment systems

The current legal framework governing ‘payment systems’ in India is given in the Payment and Settlement Systems Act 2007 (“PSS Act”). Under this law, the Board for Regulation and Supervision of Payment and Settlement System Regulations (“BPSS”), with the assistance of the Department of Payments and Settlement Systems (“DPSS”), is in charge of discharging the regulatory functions vested in RBI. The PSS Act empowers RBI to issue directions to regulate the operation and management of payment systems. A ‘payment system’ as defined under the PSS Act is “a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them.” Therefore, settlement of a payment obligation on behalf of a payer (based on an instruction by the payer) to a beneficiary, amounts to operation of a ‘payment system’. Operating a payment system in India requires a valid authorisation from RBI under the PSS Act, while operating an unauthorised ‘payment system’ attracts onerous penal provisions under the PSS Act. It is punishable with (a) imprisonment for a term which ranges from a minimum of 1 (one) month to 10 (ten) years; (b) fine upto INR 1,00,00,000 (Rupees one crore), with a further fine which may extend to INR 1,00,00,000 (Rupees one lakh) for every day that the contravention continues; or (c) both (a) and (b).

Customer identification and authentication

The RBI (Know Your Customer (KYC)) Directions, 2016 (“KYC Master Direction”) requires entities such as banks, non-banking financial companies (“NBFCs”) and pre-paid payment instrument (“PPI”) issuers...
Digital Technology Policy for India’s USD 5 Trillion Economy | 51

Digital payment intermediation

In 2009, RBI took note of the rising popularity of digital modes of payment and followed suit by issuing the ‘Directions for opening and operation of accounts and settlement of payments for electronic payment transactions involving intermediaries 2009’ ("Intermediary Directions")381. The Intermediary Directions regulate entities (such as payment aggregators and payment gateways) which facilitate digital payments by collecting funds from customers (through electronic modes of payment) for onward settlement to merchants382. These intermediaries are not classified or regulated as ‘payment systems’ and therefore do not require any authorisation or license from RBI under the PSS Act. The RBI highlighted that as standard practice, intermediaries were crediting funds (collected on behalf of customers) to their own bank accounts, before onward settlement to merchants383. Therefore, any delay or failure by the intermediary to transfer funds from its own account to the merchant posed a risk to the entire payment facilitation system. In order to contain this risk, the Intermediary Directions require entities classified as intermediaries to pool funds collected from customers in an account maintained with a bank384. These funds must be settled to merchants within a maximum of three days385 from ‘completion of transaction’386. The account in which funds are pooled is considered as an internal account of the bank, from which the intermediary cannot draw out any amounts apart from its commission387. The Intermediary Directions have not been updated or amended by RBI since 2009.

380 In case of payments to merchants which do not involve transfer of funds to nodal account, settlement must be effected within 2 (two) days of ‘completion of transaction’.
PPI as a mode of digital payment

The RBI has issued the ‘Master Direction on Issuance and Operation of Prepaid Payment Instruments’ (“PPI Guidelines”), which governs the issuance and operation of PPIs. The PPI Guidelines define a PPI as a payment instrument that facilitates purchase of goods and services ‘against the value stored in such instruments’.

Therefore, a PPI is an instrument which, (a) holds a prepaid amount as stored value, and (b) facilitates money transfers and spends from such stored value for purchase of goods and services from participating merchants. Only entities with prior authorisation from RBI are permitted to issue and operate payment systems for issuance of PPIs. A semi-closed system of prepaid payment instrument ("Semi-closed PPI") is a type of PPI defined under the PPI Guidelines. A Semi-closed PPI permits spends at participating merchants i.e. merchants with which the PPI issuer has entered into agreements.

Security framework and measures:

The PSS Act mandates all applicants of payment systems to have suitable security frameworks in place to receive an authorization to operate payment systems, failing which RBI may not grant authorization.

Presently any data classified as ‘sensitive personal data or information’ is protected against breaches of privacy, confidentiality and security under the Information Technology Act, 2000 ("IT Act"), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") framed under it. Sensitive personal data or information under these rules includes financial information.

Customer grievance and redressals

Currently, consumer grievance and redressals are governed by a number of guidelines and notifications issued by RBI under Section 18 read with Section 10(2) of the PSS Act. The RBI also released the Digital Transactions Ombudsman Scheme 2019 ("DTO Scheme") recently which provides recourse for grievances associated with ‘digital transactions’, i.e. a payment transaction made through digital / electronic modes. Pursuant to the scheme, RBI may appoint one of its officers as an ombudsman for digital transactions. A complaint may be filed free of cost with the ombudsman.

---

389 Para 2.3, Reserve Bank of India, the Master Direction on Issuance and Operation of Prepaid Payment Instruments: "Prepaid Payment Instruments (PPIs): PPIs are payment instruments that facilitate purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments."
392 Section 43A, the Information Technology Act, 2000.
393 Rule 3, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
395 Para 3(5), Reserve Bank of India, Digital Transactions Ombudsman Scheme, 2019: “digital transaction' means a payment transaction in a seamless system effected without the need for cash at least in one of the two legs, if not in both. This includes transactions made through digital / electronic modes wherein both the originator and the beneficiary use digital / electronic medium to send or receive money.”
Establishing the NPCI

The RBI and the Indian Banks’ Association (“IBA”) together formed the National Payments Corporation of India (“NPCI”), a not-for-profit entity, to act as an umbrella organisation for operating retail payments and settlement systems in India. The NPCI functions with an intention to provide infrastructure to the entire banking system in India for physical as well as electronic payment for achieving greater efficiency in operations and widening the reach of payment systems. It operates the most widely used payment systems in the country such as the Aadhaar-enabled Payments System, the RuPay cards network as well as the Unified Payments Interface (“UPI”) amongst others. UPI is by far the fastest growing mode of digital payments and merges several banking features, seamless fund routing and merchant payments into a single application. It also caters to the “peer to peer” collect request which can be scheduled and paid as per requirement and convenience.

Watal Committee Report

On 09 December 2016, a committee on digital payments led by former finance secretary Mr. Ratan P. Watal (“Watal Committee Report”) submitted a report with recommendations to promote digital payments in the country. The Watal Committee Report recommended that payment regulation should be independent of the function of central banking.

The RBI’s data localisation circular

In April 2018, the RBI issued a notification mandating that all data related to payment systems be locally stored only in India. All payment system providers were required to comply with this notification within six months, i.e., by October 2018.

Committee on deepening of digital payments

In January 2019, the RBI constituted a high-level committee on deepening of digital payments to assess the current levels of digital payments in financial inclusion, and to suggest measures to strengthen the security of such payments and encourage their growth in India. This committee has recommended that the government should target growth in the volume of low-value, high-volume, low-cost digital transactions over the next three years.

---

RBI’s framework for regulatory sandboxes

The RBI on 18 April 2019, issued a draft framework to promote innovations and competition in digital payments through the creation of ‘regulatory sandboxes’ ("RS") and ("RS Framework")404. A RS provides a pro-competitive regulatory framework which seeks to augment new innovations in test-environments. The RS could also lead to better outcomes for consumers through an increased range of products and services, reduced costs and improved access to financial services.

Payments System and Settlement Bill 2018

On 15 August 2018, the ‘Inter-Ministerial Committee for Finalisation of Amendments to the Payments and Settlement Act, 2007’, recommended a draft law, the Payment and Settlement Systems Bill, 2018 ("PSS Bill") to replace the existing PSS Act405. The PSS Bill is currently under consideration by the government. The PSS Bill seeks to "foster competition, consumer protection, systemic stability and resilience in the payments sector406". In line with the recommendation under the Watal Committee Report, the PSS Bill provides for the establishment of an independent Payments Regulatory Board ("PRB") to regulate the payments sector407.

RBI Payment and Settlement Systems in India: Vision – 2019-2021408

The recently released vision document of RBI outlines the roadmap for digital payments in India from 2019 to 2021. Its aim is to improve customer experience, empower payment system operators, formulate forward-looking regulation, enable the payments ecosystem and undertake risk-focused supervision. It consists of thirty-six action points and twelve outcomes that it hopes to achieve through the goalposts of competition, cost-effectiveness, convenience and confidence.

---

C. RECOMMENDATIONS

1. Lower regulatory barriers to entry

The PSS Act’s ambiguous and singular definition of ‘payment systems’ creates confusion on whether entities that merely provide payment technology platforms qualify as payment systems, and therefore require RBI authorisation under the PSS Act, or not. Moreover, the PSS Act provides a cumbersome process, heavy penalties and strict reporting requirements before authorizing the operation of payment systems. As a result, not only do market participants and new businesses not have clarity on the nature of authorization that they need from RBI and the kind of services that they can offer, but they are also burdened with onerous regulatory compliances. Therefore, the law must define payment systems more narrowly and classify various payment systems currently operational in the country. Additionally, it must also differentiate between payment systems and technology service providers which do not require authorisation from RBI under the PSS Act. UK law, for example, has different regulatory standards for (a) operators of payment systems, (b) payment service providers, and (c) infrastructure providers. In fact, the Watal Committee Report also suggested that the parent law classify each participant in payment systems on the basis of the service provided.

2. Adopt industry-led standards for non-systemically important payment systems

The PSS Act’s singular definition of ‘payment systems’ disallows the identification of critical payment systems that require higher security standards. Consequently, payment systems that are not systematically important and do not pose a risk to the financial market infrastructure are made to go through the same level of compliance as those which may pose a fundamental risk to the payment ecosystem. Such non-systemically important payment systems should be exempted from adopting higher security standards and corresponding compliances. This will help new businesses reduce cost and create flexibility in operations. Market participants should be allowed to develop their own self-regulatory mechanism and code of good practices to address security concerns arising in their networks.

---

409 Section 2(1)(i), the Payment and Settlement Systems Act, 2007.
410 For example, recently in March 2019, the Delhi high court sent a notice to the Reserve Bank of India and Google India enquiring about the operation of Google Pay in the country without an express authorization; Press Trust of India, How Is Google’s G-Pay Operating Without Authorisation: Delhi HC Asks RBI, available at https://www.livelaw.in/news-updates/googles-gpay-operating-without-authorisation-delhi-hc-rbi-144187. In this instance the court must consider that Google Pay operates as a technology service provider to its partner banks to facilitate payments through the unified payment interface infrastructure. It is not part of payment processing or settlement and therefore does not require Reserve Bank of India authorisation as a payment system under the Payment Settlement Systems, Act. T. Bhalla, Google Pay responds to Delhi HC notice on operating without authorisation, available at https://yourstory.com/2019/04/google-pay-response-delhi-hc-notice.
3. Create clarity under the RS framework

The RS Framework envisages strict eligibility criteria for businesses to participate in the regulatory sandbox. Only 'start-ups' (according to DPIIT’s definition of the term413) will be considered for the sandbox414. These criteria must be revised to also include other entities that do not qualify as ‘start-ups’ as defined by DPIIT. Customer adoption under the RS environment may be more effective if such entities with a critical mass of users are permitted to participate in the RS environment. Further, the RS Framework does not contemplate the role of licensed payment systems such as banks. Their role is in fact critical, given that many participants in the regulatory sandbox environment may not be directly regulated by RBI. Further, since the RS Framework does not exempt participants from regulatory requirements such as data privacy415 and consumer protection416, start-up entities may not have mechanisms in place to meet these levels of compliance. In addition, a buy-in from licensed entities may also be needed given that several fin-tech products and innovations are developed by unlicensed entities which have entered into contractual relationships with licensed entities to provide financial products to users. Moreover, one the key objectives of the RS Framework must be to effect policy change based on the observations made in the RS environment. If a product/service introduced here demonstrates commercial viability without compromising overall system security, RBI must consider issuing tailored or relaxed guidelines governing like products/services. This would dovetail into the larger goal of promoting competition, which would spur innovation and expand consumer choices.

4. Relax AFA for recurring transactions

The RBI currently requires an additional factor authentication (“AFA”) on card not present transactions (“CNP Transactions”)417. This mandate also applies to all recurring transactions based on standing instructions given to the merchants by the cardholders. This creates an additional layer of friction and especially hurts subscription-based businesses418. While RBI relaxed the AFA in 2016 for small-ticket transactions up to INR two thousand419, it is still unclear whether the AFA requirement has been completely done away with for such transactions, or if it has simply become the domain of card network providers. In order to promote subscription-based businesses, RBI must consider relaxing the AFA requirement for CNP transactions where a cardholder has set up a standing instruction with a merchant. The cardholder should be asked to undertake an AFA only once: at the time of setting up the standing instruction, post which the merchant could inform the cardholder before each impeding payment with an option to opt out of making such payment. Therefore, the user must not be required to conduct AFA to approve each successive payment transaction after setting up the standing instruction.
5. Simplify KYC norms for PPIs

PPIs are required to undertake the same level of KYC as banks. Semi-closed PPIs with credit limit up to INR ten thousand require the holder to have completed KYC (as contemplated under the Master KYC Directions) within a period of eighteen months from the date of issue of PPI\(^{420}\). Semi-closed PPIs with credit limit up to INR one lakh require full KYC at the time of issuance\(^{421}\). This does not make a PPI an attractive digital payment option for small value transactions, creates friction, and has limited usage. Further, specifically where funds to a PPI are loaded through a KYC verified account i.e. debit to a bank account, credit and debit cards, the need for a dual KYC at the time of issuance of the semi-closed PPI seems unnecessary. The additional cost of undertaking a full KYC for PPIs deters payment solution provider from promoting PPIs over other payment mechanisms. The RBI must allow simpler and digital KYC processes to incentivise PPI issuers to promote PPI as a viable payment option. It must also reduce the level of KYC required to issue semi-closed PPIs. Simplifying KYC norms will also drive interoperability between PPIs.

6. Adopt global standards for security by design

Each payment system is exposed to various risks like credit, liquidity, legal, operational and settlement risks\(^{422}\). In India, Cosmos Bank was faced with a cyberattack, resulting in nearly INR 1,00,00,000 (Rupees one crore) being siphoned off. The security breach in ATMs in 2016 compromised debit cards details of the consumers and allowed fraudsters to access confidential debit card data from ATM networks. The RBI investigated the incident which allowed the miscreants to steal personal information and misuse the data on the card for fraudulent transactions\(^{423}\). The systemically important payment systems should incorporate security-by-design principles that adhere to global standards for information and network-security protocols\(^{424}\). Advanced cyber-security jurisdictions such as Singapore\(^{425}\) and the United Kingdom\(^{426}\), in their respective cyber-security strategies, seek to promote security-by-design principles in the digital ecosystems. TRAI has also endorsed standardisation against security-by-design benchmarks\(^{427}\). In addition, the current security standards in India lack device-level cyber-security standards and follows outdated information-security benchmarks. As digital payments are most accessed with the use of mobile devices, the devices should adopt integrated security mechanisms against layered defences\(^{428}\).

---


7. Incentivise digital payments

India’s dependence on cash is acute, with the total cash flow in the market estimated to be around 12 per cent of our GDP, which is amongst the highest in developing countries. In order to address this, the government must encourage the adoption of digital payments while also dis-incentivising cash transactions. Introducing tangible benefits such as income tax incentives based on digital transactions for individuals, and Goods and Services Tax credits for merchants based on the volume of digital payments accepted, surcharge removal and subsidies on merchant discount rates on government payments like taxes, tolls and utility bills could help a large chunk of payments go digital. Allowing non-bank PPI issuers to earn interest on the entire balance funds lying in their escrow account and removing the restriction that interest can only be earned after one year from the issuance of the PPI license will incentivise the promotion of PPI. Cash transactions could be dis-incentivised by imposing nominal charges after a certain limit to encourage consumers to shift towards digital payments. Similarly, quarterly or yearly limits on cash transactions could also be introduced. The government may also consider gradually reducing the threshold for quoting the PAN for cash transactions in banking from INR 50,000 and for similarly for merchant/other transactions where the current threshold is INR 2,00,000. Allowing PPI holders to earn interest on funds lying in their PPI accounts will also encourage the shift away from cash transactions.

8. Better customer protection frameworks

Creating and protecting consumer trust is a key issue in provision of payment service, and the absence of strong laws protecting consumers is a problem. Consumers must be effectively informed about terms and conditions of digital service, the risks associated with a service, and liability in case of unauthorised access, among other things. To empower consumers, the payments regulator must take a consumer-centric approach when developing and expanding the Indian digital payments market. Consumer protection is too important an issue to be left to the discretion of any regulatory agency. Instead, the broad principles for consumer empowerment need to be hardwired into statutory laws with clear accountability to enable a regulatory shift towards consumer-centric approach. A large number of people are still illiterate in India and can be victim of fraud or other malpractices while using digital payment options. Many street vendors and shopkeepers still struggle to adopt swipe machines and other digital payment modes. There is a need to promote ease of adoption by including multi-lingual financial literacy and a robust grievance redressal machinery to effectively handle inter-regional disparities and offer online dispute resolutions.

---

432 Para 12.4(c), Reserve Bank of India, the Master Direction on Issuance and Operation of Prepaid Payment Instruments, dated 11 October 2017, available at https://rbi.org.in/ScriptS/BS_ViewMasDirections.aspx?id=11142. It allows non-bank PPI license issuers to earn interest on the entire balance funds lying in their escrow account and removing the restriction that interest can only be earned after one year from the issuance of the PPI license.
433 Para 12.4, Reserve Bank of India, the Master Direction on Issuance and Operation of Prepaid Payment Instruments, dated October 11 2017 available at https://rbi.org.in/ScriptS/BS_ViewMasDirections.aspx?id=11142. It allows non-bank prepaid payment instrument issuers to earn interest only on an amount calculated as the ‘core portion’.
436 The minimal transaction fees earns by PPI issuers are an inadequate incentive for promotion of PPI as a payment instrument. An additional interest earning is essential for PPI issuers to promote and invest in the PPI business.
438 With rapid innovation in the digital payment industry and the introduction several frictionless digital payment platforms, ‘ease of use’ may no longer be an adequate incentive for use of PPIs.
442 Para 12.4, Reserve Bank of India, the Master Direction on Issuance and Operation of Prepaid Payment Instruments, dated 11 October 2017, available at https://rbi.org.in/ScriptS/BS_ViewMasDirections.aspx?id=11142. It allows non-bank prepaid payment instrument issuers to earn interest only on an amount calculated as the ‘core portion’.
445 The minimal transaction fees earns by PPI issuers are an inadequate incentive for promotion of PPI as a payment instrument. An additional interest earning is essential for PPI issuers to promote and invest in the PPI business.
447 With rapid innovation in the digital payment industry and the introduction several frictionless digital payment platforms, ‘ease of use’ may no longer be an adequate incentive for use of PPIs.
9. **Create an independent supervisory board for regulating payment systems**

The establishment of a PRB could create dual and overlapping regulatory oversight of various financial products and services. There is a need for transparency in how the proposed independent board will function. While there may be a need to create a PRB to foster competition and consumer protection, and to create systemic stability and resilience in the payments sector. In order to avoid overlapping regulatory oversight, RBI must nominate a certain percentage of the board members to the PRB. Further, the PRB’s consultation with RBI must be mandatory before any new framework governing financial products and services is issued. These steps may ensure better synchronisation between RBI and PRB in the decision-making process.

10. **Promote interoperability between digital payments’ interfaces**

Both the introduction of UPI and the RBI’s ‘Prepaid Payment Instruments (PPIs) – Guidelines for Interoperability’ ("RBI Interoperability Guidelines") have contributed immensely to promoting interoperability between digital payments’ interfaces. We believe that the government should give impetus to the implementation of the RBI Interoperability Guidelines to further enhance digital payment interoperability in the country. Additionally, generating awareness around the feature of interoperability between myriad digital payments’ systems will also contribute to the creating a cashless economy.

11. **Reform the NPCI**

The role and structure of the NPCI should be revisited. The NPCI owns and operates several retail payment and settlement systems in India, including RuPay and the Bharat Interface for Money (”BHIM”) which is a UPI application. This puts it in competition with other private technology payment players in India. At the same time, the NPCI is also the rule making body for UPI in India, which allows it to regulate all UPI applications in the country. This is a conflict of interest, which should be addressed as soon as possible. Moreover, concerns have been voiced around the neutrality of the NPCI. For instance, in the 2018-19 budget, INR 595 crores were earmarked for the digital payments sector, of which the NPCI allocated INR 495 crores to BHIM, instead of splitting it equally across all UPI players. In similar vein, since a majority stake of the NPCI is owned by public sector banks, private financial technology companies may not be adequately represented. These issues may be addressed by separating the regulatory and operational functions of the NPCI or by creating an NPCI like institution to take over the NPCI’s regulatory functions. Further, the government may explore regulatory checks on NPCI or introducing measures to enhance the transparency in the workings of the NPCI to address any concerns around NPCI’s neutrality.

12. **Enhance industry participation to realise RBI’s vision on digital payments**

The RBI released the ‘Payment and Settlement Systems in India: Vision – 2019-2021’ document ("RBI Vision Document") on 15 May 2019 to enhance the penetration of digital payments in India. We believe the government should increase industry participation to create a roadmap with clearly-defined, time-bound goals to ensure that the objectives of the RBI Vision Document are met on the ground.
PLATFORM REGULATION: INTERMEDIARY LIABILITY

A. Context

Online platforms including e-commerce marketplaces, payment companies, video platforms, messaging platforms, blogs and social media platforms, amongst others, add substantial value to the economy by creating globalised marketplaces, offering new modes of distribution of products and services, lowering transaction costs, and fostering competition. These platforms do not create their own content but only act as intermediaries for third parties. In India, these intermediaries are not held liable for any illegal act or content on their platform provided they observe certain due diligences. This protection is called 'safe harbour' protection. Safe harbours need to be protected and strengthened because they bolster the digital economy, enhance internet penetration, increase the competitiveness of companies, and promote innovation.

In India, internet intermediaries are governed by the Information Technology Act, 2000 (“IT Act”) and the rules framed under it. Key among these rules are the Information Technology (Intermediary Guidelines) Rules, 2011 (“Intermediary Rules”). The Supreme Court in Shreya Singhal v. Union of India (“Shreya Singhal Case”) clarified the contours of this legal framework.

In 2018, the government released the Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 (“Draft Intermediary Guidelines”) which propose to increase due diligence standards. The Telecom Regulatory Authority of India is deliberating recommendations for regulating over-the-top (“OTT”) platforms, who qualify as intermediaries under current law.

B. Current state of law and policy

An intermediary is any entity that receives, stores or transmits information on behalf of third parties. Safe harbour protection is extended to intermediaries on the basis of the principle that they are passive transmitters of information and have little to no control over the same. To avail safe harbour protection, intermediaries must inter alia publish the rules and regulations governing the use of their platform by users and explicitly prohibit the use of their platforms to publish or transmit certain kinds of data.

---


446 The Information Technology Act, 2000. Section 79, Information Technology Act, 2000 lays down the requirements for intermediaries to avoid liability.

447 The Information Technology (Intermediary Guidelines) Rules, 2011.


451 Section 2(w), the Information Technology Act, 2000.

452 Rule 3(1), the Information Technology (Intermediary Guidelines) Rules, 2011.

453 Rule 3(2), the Information Technology (Intermediary Guidelines) Rules, 2011.
They should also not “initiate the transmission, select the receiver of transmission, and select or modify the information” on their platforms and must remove certain kinds of content from their platforms upon being notified of the same, amongst other due diligences. In the Shreya Singhal Case, the Supreme Court held that an intermediary was to take down content only upon receiving “actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed” (“actual knowledge”). However, in a later judgment the Delhi High Court held that in case of copyright infringement, a judicial or administrative order was not necessary.

Further, the criteria for determining when an intermediary is a passive transmitter of information and amenable to safe harbour protection as opposed to when an intermediary is an active transmitter of information and not amenable to safe harbour protection is increasingly becoming blurred.

The Draft Intermediary Guidelines, released last year, propose setting up a local Indian company for certain intermediaries, providing assistance to government agencies, removing certain content from their platforms, deploying automated tools to proactively filter content, and enabling tracing of senders of certain content amongst others.

Not only intermediary liability, but the regulation of content on online platforms is in itself also a contentious issue. Last year in Justice for Rights Foundation v. Union of India (“JRF Case”), the petitioner requested the Delhi High Court to formulate guidelines for the regulation of online content. However, the Delhi High Court refused to do so and left the regulation of online content to the IT Act and the rules framed under it. At the same time, we have seen the evolution of co-regulation and self-regulation, with several OTT players such as Netflix, Hotstar, Viacom, ALTBalaji, amongst others coming together and subscribing to a voluntary online code for online content (“Online Content Code”).

---

454 Rule 3(3), the Information Technology (Intermediary Guidelines) Rules, 2011.
455 Rule 3(4), the Information Technology (Intermediary Guidelines) Rules, 2011.
456 Rules 3(5) to 3(11), the Information Technology (Intermediary Guidelines) Rules, 2011.
457 Rule 3(4) was interpreted to mean only knowledge through a court or administrative order.
458 Para 6, Justice for Rights Foundation v. Union of India, W.P(C) 11164/2018, Delhi High Court.
467 Justice for Rights Foundation v. Union of India, W.P(C) 11164/2018, Delhi High Court.
468 Para 6, Justice for Rights Foundation v. Union of India, order dated 08 February 2019, W.P(C) 11164/2018, Delhi High Court.
469 The Online Content Code was formulated in collaboration with the Internet and Mobile Association of India and prohibits certain kinds of content, provides guidelines on content classification, and suggests the appointment of a person/team/department for grievance redressal. The text of the same is available at https://www.medianama.com/wp-content/uploads/Consolidated-Draft-14012019.pdf.
C. RECOMMENDATIONS

1. Preserve safe harbour protection

Strong safe harbour provisions promote innovation and entrepreneurship as seen in the US\(^{470}\) while diluting safe harbour provisions detrimentally impacts end user experience and range of choices. Safe harbours enable the freedom of expression which in turn fuels creativity\(^{471}\) and innovation\(^{472}\). Weak safe harbour protection will discourage fresh investment\(^{473}\) as well, which will affect the government’s efforts to create a vibrant start-up culture. In order to achieve the vision of the ‘Digital India’ programme, India must preserve its safe harbour protections. Therefore, the existing safe harbour protection under Section 79 of the IT Act must be strengthened. Given the number of sectors that different intermediaries operate in, it must be clarified that sector-specific laws and regulators cannot be involved in determining questions of intermediary liability, as such questions must be tackled within the contours of the IT Act. Additionally, the Draft Intermediary Guidelines should not be implemented in their present form as they impose a number of onerous obligations on intermediaries. Additionally, they also contravene the judgment in Shreya Singhal by imposing proactive monitoring and takedown requirements\(^{474}\), amongst other onerous conditions.

2. Do not introduce pro-active content monitoring requirements

The Draft Intermediary Guidelines\(^{475}\) require intermediaries to pre-screen content through automated means\(^{476}\). This deviates from the principle that intermediaries should be passive transmitters of information, and may lead to a loss of safe harbour protection. To prevent this from happening, companies may begin over-complying\(^{477}\) and censor legal content as well. It also goes against the Shreya Singhal Case which mandates a judicial or administrative order to take content down. Given the volume of information to be filtered, many companies may begin to deploy automated tools. These are also error-prone\(^{478}\) and have seen limited success\(^{479}\). Sub-standard tools may censor even legal content. All this is likely to have a chilling effect on free speech and expression which is a constitutionally protected right. Therefore, the Draft Intermediary Guidelines must be revisited.

---

470 A. Chander, ‘Internet Intermediaries as Platforms for Expression and Innovation’, Global Commission on Internet Governance: “Imagine the boardroom in a Silicon Valley venture capital firm, circa 2005. A start-up less than a year old... Now that start-up... needs an infusion of cash to survive and grow... If that start-up can be accused of abetting copyright infringement on a massive scale, or must police its content like a traditional publishing house, lest it face damages claims or an injunction, the firm’s US$100 million investment might go to plaintiffs’ lawyers in damages and fees. A court injunction might stop the site from continuing without extensive human monitoring, which could not be justified by potential revenue. Because of the insulation brought by US law reforms in the 1990s, American start-ups did not fear such a mortal legal blow. The legal privileges granted to Internet enterprises in the United States helped start-ups bridge the so-called “valley of death,” the stage between creative idea and successful commercialization, in which most start-up enterprises founder.” See https://www.cigionline.org/sites/default/files/documents/GCG%20no.42.pdf.


477 N. Pahwa, #NAMApolicy on Safe Harbor: Should different sizes or categories of intermediaries be regulated differently?, available at https://www.medianama.com/2019/02/223-regulation-of-intermediaries-nama/?fbclid=IwAR1IUx2a20Gc2cGby04lQaLiNJH6Big7B5H3eTxr22a2QUPF6ozOyd7Q.


479 In Sabu Mathew George v. Union of India, (2017) 7 SCC 657, it was submitted by the respondent intermediaries that content which violated the PCDNDT Act could be removed only after being brought to their notice. Even such limited blocking has not seen much success; Legally India, Roundup of Sabu Mathew George vs. Union of India: intermediary liability and the ‘doctrine of auto-block’, available at https://www.legallyindia.com/views/entry/roundup-of-sabu-mathew-george-vs-union-of-india-intermediary-liability-and-the-doctrine-of-auto-block.
3. Do not mandate intermediaries to set up registered offices in India

The Draft Intermediary Guidelines require certain intermediaries to have a registered office in India. This will increase operational costs. Certain companies may choose to not comply with this requirement and stop offering services in India. This will reduce the quality of services available to Indian citizens who will lose out on innovative online products and services. Vietnam, which has a similar requirement for the local presence of foreign-service providers, is already facing the commercial harms of this mandate. We believe that these strategic decisions should be left to market forces. The government may incentivise companies to set up companies in India instead.

4. Do not regulate content on online platforms

As the Delhi High Court has recognised in the JRF case, the IT Act is sufficiently equipped to deal with the regulation of online content. Therefore, online platforms should be allowed to function within the bounds of the IT Act and its frameworks, as well as supplementary self-regulatory/co-regulatory models.
A. Context

Information technology (“IT”) companies and digital businesses have grown to form a core part of the Indian economy today. From a contribution of a mere 1.2% to the national GDP in 1998, the IT sector now contributes to 8% of the national GDP. Per IT Minister Shri Ravi Shankar Prasad, this number is expected to increase manifold over the next five years, with revenues from the IT sector rising to as much as USD 350 billion.

To further aid this growth, it is important to review and reform horizontal laws like the Competition Act, 2002 (“Competition Act”) and the Income Tax Act, 1961 (“Income Tax Act”) that cut across multiple sectors of the digital economy. The constitution of the Competition Law Review Committee (“Review Committee”) by the government in September 2018 and the frequent government-driven reforms of tax laws are welcome steps in this direction.

B. Current state of law and policy

Competition law

The Competition Commission of India (“CCI”) is a relatively new regulator, which took over the task of regulating the Indian market from the Monopolies and Restrictive Trade Practices (“MRTP”) Commission in May 2009. Since the CCI has been in operation for a decade thus far, the jurisprudence on competition law is still at a nascent stage in India. During this time, the CCI has grappled with challenges like distinguishing between offline and online marketplaces, determining the effects of deep discounts on healthy competition, and the abuse of dominance by technology companies.
The CCI undertook several market surveys to understand the nuances relating to technological developments and also constituted a ‘Think Tank on Digital Markets’ ("Think Tank") comprising of technologists, legal experts and economists to help the CCI reach well-informed decisions with regards to the digital economy.

**Digital taxation**

At present, digital services are taxed on the basis of the physical presence of an entity within the taxing country. In February 2016, then Finance Minister Shri. Arun Jaitley proposed the introduction of an ‘equalisation levy’, that was meant to “tap tax on income accruing to foreign e-commerce companies from India”. As per the Finance Bill, 2016, this levy is to be charged on the amount of consideration paid by a person resident in India/a non-resident having a permanent establishment in India to a non-resident for any “specified service”. In May 2016, the Central Board of Direct Taxes ("CBDT") implemented this proposal by introducing an equalisation levy for taxing digital services like online advertising.

In 2018, the Income Tax Act was amended to widen the meaning of ‘business connection’, such that even entities with a significant economic presence ("SEP") in India, were considered to have a business connection within the country. With this amendment, all income that accrues or arises, whether directly or indirectly, through or from any SEP (i.e., a business connection) has become taxable in India, since such income is deemed to be income that accrues or arises in India.

---


499 Explanation 2A to section 9, Income Tax Act, 1961: “Explanation 2A.—For the removal of doubts, it is hereby clarified that the significant economic presence of a non-resident in India shall constitute "business connection" in India and "significant economic presence" for this purpose, shall mean—(a) transaction in respect of any goods, services or property carried out by a non-resident in India including provision of download of data or software in India, if the aggregate of payments arising from such transaction or transactions during the previous year exceeds such amount as may be prescribed, or (b) systematic and continuous soliciting of business activities or engaging in interaction with such number of users as may be prescribed, in India through digital means.”

In early 2019, the Draft National E-commerce Policy discussed the problems associated with imposing a permanent moratorium on custom duties on electronic transmissions. Most recently, the CBDT constituted a committee to look into the manner of attributing profits to permanent establishments under the Income Tax Act, 1961. On 18 April 2019, the committee released a proposal for amending the rules on profit attribution to a permanent establishment, inviting stakeholder comments on the same. The government’s decision on the way forward on this issue will have a significant impact on digital businesses operating in India.

C. RECOMMENDATIONS

Competition law

1. Incentivise participation of experts in the Think Tank and invest in capacity building:

The success of the Think Tank approach is contingent on the presence of skilled experts in the Think Tank and the methodology of their research. The CCI should initiate a call for participants with technical expertise for the Think Tank for better results. Additionally, it can encourage internal capacity building in collaboration with industry stakeholders so that persons remain up to date with the developments on the technology landscape.

2. Increase transparency in internal processes

The process of selecting members for the Review Committee, the Think Tank as well as the market surveys were not made available to stakeholders for review. Further, the findings of these bodies have not been made publicly available. It is therefore recommended that the CCI should increase transparency in the way it structures these bodies/exercises and conducts its own functions. In addition, the CCI should ensure that stakeholder consultations on key issues take place.

3. Update the Competition Act

The Competition Act is still evolving to address the issue of the growing digital economy. The Act still pegs the definition of a ‘market’ to its geographical or product market, which may not be suited to the e-commerce marketplace where physical presence is not a pre-requisite for doing business. This outlook has impact edits decision in Mohit Mangalani v Flipkart India Private Limited (2014). The CCI instituted the Review Committee to propose amendments to the Act, yet no recommendations have been given yet. The Review Committee must be directed to submit its report at the earliest.

---

506 Mohit Mangalani v Flipkart India Private Limited, Case No. 80 of 2014.
4. **Consider the introduction of settlement proceedings**

The pace of decision making by the CCI is not up to speed with the rapid changes in the digital economy. By the time a final decision is pronounced, digital economy market conditions change drastically\(^{507}\). Settlements have become a widely accepted mode of dispute resolutions in many major economies of the world, including the US\(^{508}\) and the European Union\(^{509}\). They enable competition authorities to save resources which leads to the swifter resolution of cases\(^{510}\). Further, since settlements entail a process of negotiation, competition authorities can create custom-made remedies suitable for the particular facts of each case\(^{511}\). Most importantly, settlements can enable a quicker restoration of effective competition in markets\(^{512}\). Given these myriad benefits, the government should seriously consider introducing settlement proceedings within the framework of the Competition Act.

**Digital taxation**

1. **Apply new rules prospectively**

The government must ensure that all new rules and other developments affecting taxation are applied prospectively. It should specifically be clarified that such instruments have no bearing on ongoing assessments or appellate proceedings.

2. **Adopt a balanced approach to amending India’s tax framework**

Developments such as the introduction of the SEP principle, introduction of an equalisation levy and deliberations on the customs moratorium on electronic transmissions require in-depth and careful consideration by all stakeholders, as they replace settled international norms. International organisations such as the Organisation for Economic Cooperation and Development are yet to make their final recommendations on these issues. Any decision on this matter will have a ripple effect throughout the Indian economy. It is therefore important for the government to adopt a balanced approach to decision-making on issues such as digital taxation, as they impact global inter-connectedness, which brings many positive returns to the Indian GDP.

3. **Honour existing Advance Pricing Agreements**

Advance Pricing Agreements ("APA") have been signed and executed by the CBDT with several taxpayers. These APAs, particularly those related to marketing activities performed by Indian entities, have addressed the attribution risks for non-residents. It is unclear how the recommendations suggested by the CBDT would integrate with these signed and executed APAs. Therefore, an exception should be carved out for non-residents already covered by the APA program.

---


1. Where the Commission intends to adopt a decision requiring that an infringement be brought to an end and the undertakings concerned offer commitments to meet the concerns expressed to them by the Commission in its preliminary assessment, the Commission may by decision make those commitments binding on the undertakings. Such a decision may be adopted for a specified period and shall conclude that there are no longer grounds for action by the Commission.

2. The Commission may, upon request or on its own initiative, reopen the proceedings:

(a) where there has been a material change in any of the facts on which the decision was based;

(b) where the undertakings concerned act contrary to their commitments; or

(c) where the decision was based on incomplete, incorrect or misleading information provided by the parties.”


