[Un]Ease of Doing Digital Business in India

A Study of Policy and Regulatory Challenges

CUTS International

#2212

[Un]Ease of Doing Digital Business in India

A Study of Policy and Regulatory Challenges

CUTS International

[Un]Ease of Doing Digital Business in India

A Study of Policy and Regulatory Challenges

Published by

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Citation:
CUTS International, [Un]Ease of Doing Digital Business in India: *A Study of Policy and Regulatory Challenges* (Jaipur 2022).

#2212

Author's Profile

Neelanjana Sharma

Neelanjana is a policy researcher working with Consumer Unity & Trust Society (CUTS) International as a Senior Research Associate. At CUTS she deals with issues largely concerned with the digital economy, specifically digital rights, privacy, financial inclusion, data protection. She has previously worked with six state governments as a legal consultant and advisor. She is a law graduate from Nirma University, Ahmedabad and has a LLM specialisation in Constitutional and Administrative Law.

Asheef Iqubbal

Asheef Iqubbal is a Senior Research Associate with Consumer Unity and Trust Society and works at cross-sections of technological governance, digital economy, and socio-economic justice. At CUTS, his work focuses on data governance, e-commerce, and telecom. He has previously worked as a policy researcher with a New Delhi-based not-for-profit organisation. Asheef has done his engineering from Maharishi Dayanand University, Rohtak.

Prince Gupta

Prince Gupta is a technology law and policy researcher who works as a Senior Research Associate at Consumer Unity & Trust Society (CUTS) International. He deals with issues related to digital rights like data privacy and data protection, information disorder, telecom policy and regulation and competition issues in the digital economy at large. He is an engineering graduate from Vellore Institute of Technology, Chennai and has a Masters in Public Policy from the National Law School of India University, Bangalore.

Contents

Foreword

RITESH PANDEY
Member of Parliament (Lok Sabha)
Ambedkar Nagar, Uttar Pradesh

CHAIRPERSON
Committee on Papers Laid on the Table
Lok Sabha

सत्यमेव जयते

Member:
Standing Committee on External Affairs
Consultative Committee - M/o Power,
Ministry of New & Renewable Energy

Foreword

The COVID-19 pandemic has increased our dependency on digital technologies. To cater to the needs of the people, the Indian government must facilitate a digital revolution and increase digital connectivity so that digital businesses can contribute towards betterment of the lives of people. Technology-led growth can be a pillar of India's economic growth if the government offers support for technological innovations. However, the government's push for regulatory reforms for the digital ecosystem and enhanced technological infrastructure has not been in tandem with the principles of liberty and justice.

The government should adopt consultative and participatory law making process which will produce confidence of all the stakeholders in digital spaces. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, for example, raised multiple concerns including on encryption and putting disproportionate responsibilities on businesses that can potentially endanger privacy.

Consumer Unity and Trust Society's (CUTS') study on 'Ease of Doing Digital Business' is an important and timely intervention that brings attention to factors impacting digital businesses. The report, '*[Un]Ease of Doing Digital Business: A Study of Policy and Regulatory Challenges*' has underpinned some significant concerns such as the presence of unnecessary compliances and regulatory uncertainty that digital businesses are facing. The report correctly states that the delays in enacting data protection legislation has caused increasing uncertainty for businesses.

The government has withdrawn the Data Protection Bill, 2021 (DPB) for which extensive resources were put in. Policymakers should draw learnings from the process undertaken with respect to Joint Parliamentary Committee's (JPC) reports and consultations in which civil society organisations actively participated. The report highlights critical points related to the DPB. The government can utilise suggestions made in the report for ensuring the independence of any future Data Protection Authority. Also, in regulating non-personal data, the government seemed to be in a hurry and that might be counterproductive when the market is not mature.

In the Finance Bill 2022, the government had put one percent Tax Deducted at Source (TDS) on all crypto transactions which has had negative implications on the sector. Rather than enabling the environment, the government is strangulating all the crypto transactions. Underscoring regulatory impact on cryptocurrencies, the report aptly states that the government has adopted an inconsistent approach which has created uncertainty for both, industries as well as consumers, terming the regulation 'arbitrary'.

Furthermore, the report rightly emphasises on making the digital economy more inclusive by taking concerns of smaller businesses into account as the digital businesses have presented nuanced regulatory and policy challenges. In order to promote innovation and investment for digital businesses in India, further studies as well as governmental attention is needed.

Ritesh Pandey,
Member of Parliament, Lok Sabha

201, Block-B, Parliament House Annexe Extension Building, New Delhi-110 001
Tel.:011-23035738, Fax: 011-21410273
E-mail: office@riteshpandey.in, ritesh.pandey@sansad.nic.in

Acknowledgement

Several people have contributed to the success of this report in various forms by providing direct inputs, discussions, reviews, encouragement and guidance. We are grateful to Amol Kulkarni, Director (Research), CUTS International for his constant encouragement, guidance and faith in the team.

During the study, we wish to extend our regards to the digital startups that provided us with insights and gave us their valuable time. These include WaahShop, GoingZero, Effectization Studio, Tinkerly, and Bodhi Sattva AI. Our research benefited from the inputs from Ms. Beni Chugh of Dvara Research, Ms. Zainab Bawa of Hasgeek, and Nehaa Chaudhari of Ikigai Law.

We extend our regards to Kapil Gupta (Former Assistant Policy Analyst, CUTS International), Aparna Choudhary (Former Policy Analyst) and Jainisha Bhanawat (Former Research Associate) for their support and initial conceptualisation of the study.

We appreciate the efforts of Akshay Sharma and Ritu Sharma (Programme Team), and Sweepthish Jayan and Keval Sharma (Information Technology Team). We sincerely thank Madhuri Vasnani, Rajkumar Trivedi and Mukesh Tyagi (Publications Team) of CUTS International for their exemplary support in making this report become a reality.

We express our sincere gratitude to all such individuals, whether or not named above, without whom the publication of this report would not have been possible. Finally, any error that may have remained is ours alone.

Neelanjana Sharma, Asheef Iqubbal and Prince Gupta

Senior Research Associates, CUTS International

Author's Note

India is steadfastly gearing towards being a digital first economy. In government, technology is driving effectiveness and efficiency while leading the way into a transformed India. The Government of India has undertaken various reforms in order to ease the environment for businesses, by developing new infrastructure and making regulations more efficient.

In view of ushering in the industrial revolution 4.0, the regulatory reforms in the country are moving towards decriminalising minor offences, reducing, simplifying unnecessary compliances, developing public infrastructure, reframing cross-border data flow restrictions, and removing regulatory uncertainty amongst others. These initiatives are the keystones in achieving new growth goals for India.

India's digital ecosystem presents a promising prospect for all digital entities as the future lies in technological disruptions. The policy makers' zeal to enhance innovation and aid technological development in India has led to the groundbreaking changes across spectrums of digital finance by means of unified payments interface (UPI) and Indiastack, but the tectonic shift is not limited to digital finance. India has become a hub for start-ups with a total of 105 unicorns in India and for further economic growth focus should be on sunrise areas. In the light of above mentioned advancements among others, the new changes to regulations and public infrastructure needed to be looked at from the perspective of whether these have enhanced the ease of doing business for digital businesses in India.

We had thus taken up the task in the form of CUTS' study on Ease of Doing Digital Business in India. The study lays ground for further focus on regulatory and policy challenges that digital businesses continue to face. These challenges range from incorporation of provisions for imprisonment of employees of digital businesses to unnecessary compliances many of which could be simplified, reduced or repealed. The rising number of digital businesses, often operating in a regulatory vacuum has not only led to uncertainty but also created entry barriers for smaller businesses. The study comes up with recommendations, inclusive of policy, systemic and in form of gentle nudges for the landscape of regulations that intends to cover the intangible nature of technological businesses.

In the end, we hope that this study becomes the first of many which looks into, poses questions and creates nudges for more efficient and inclusive regulations for the advancing age of technology and the entities that operate in it. We recognise that various developments have happened since we had taken up this task, but in view of time and relevance, we have limited our study's scope to July 2022. All the fallacies of the study remain our own.

Humbly,
Neelanjana, Asheef and Prince

1 CHAPTER Executive Summary

The Government of India (GoI) is making significant efforts towards promoting digital businesses like developing public infrastructure such as Aadhaar to boost the digital economy. Policies are increasingly being introduced with the aim of facilitating a fair, competitive and innovative environment for doing digital businesses in India. This has resulted in multiple Indian success stories including vibrant homegrown start-ups and India has become a global leader in online payment transactions, among others. Furthering digital businesses will be critical to achieving the stated aim of a US$1tn digital economy by 2025.

Ease of Doing Business (EoDB) reforms have not been in tandem with Ease of Doing Digital Businesses (EoDDB) in terms of regulatory and policy changes. While recognising the significant efforts made by the GoI in promoting digital businesses, the EoDDB initiative underscores the persisting bottlenecks in doing digital businesses to provoke further conversation in the spirit of enriching the discussion and to prompt governmental reforms around doing digital businesses, which is critical to making economic growth in digital space more inclusive.

EoDDB is important not only for businesses but also for consumers as it increases the diversity in choosing goods and services – enhancing Ease of Living (EoL). Keeping this perspective in mind, CUTS has initiated conversation on EoDDB in order to enhance the ecosystem of doing digital businesses by identifying and studying five factors — after reviewing existing literature — and their implications on digital businesses. These include *criminalising provisions, regulatory uncertainty, unnecessary compliances, inadequate digital infrastructure* and *restriction on cross-border data flow*. This has been done in tandem with stakeholders' engagement – digital businesses, experts and regulators.

The laws and regulations in India contain multiple **Criminalising Provisions** for minor economic offences and provisions of imprisonment for non-compliances with executive orders. Additionally, multiple sectors, such as e-commerce, online gaming, ed-tech and fintech, among others, are facing **Regulatory Uncertainty**. For instance, in the cryptocurrency sector, due to the regulatory uncertainty, reportedly, companies have restructured their strategies. Despite significant effort in infrastructural development, **Inadequate Digital Infrastructure** remains one of the most basic constraints, including connectivity in doing digital businesses in India.

Moreover, some compliances are disproportionate for digital businesses which need to be critically examined. **Unnecessary Compliances** increase the cost of operation for digital businesses as they have to incur the cost of consulting, chartered accountant firms or law firms. Business communities have been showing their discontent over implications and compliance-related to restrictions on **Cross-Border Data Flow**. Merits of cross-border data flow restrictions need to be evaluated as they will impact the fundamentals of digital business as well as global interdependence in the technology-led economic growth.

For engagement with digital businesses, after reviewing the digital business landscape and bottlenecks, 15 digital businesses were identified on the basis of sector, scale and relevance for the project. A team of researchers conducted semi-structured, in-depth interviews of these businesses. Further, interaction with experts was done to validate and gauge a holistic understanding of challenges in doing digital businesses in India.

All the data was aggregated and analysed to develop nuances of the bottleneck that digital businesses are facing. Interviews with key stakeholders helped to fill the gaps in publicly available information and provide a deeper understanding of the implications of policies, regulations and infrastructure in doing digital business in India. The study aims to inform policymakers and the business community of the shortcomings of policies and their implications on EoDDB and to impel governmental reforms for EoDDB. To this end, each Chapter, which focuses on five above-mentioned factors, has made **suggestions** for them to consider.

The key findings and recommendations of the study are as follows:

Criminal Liability

Key Findings

In this Chapter, we have assessed regulations and laws targeted towards digital businesses which contain criminalising provisions. Section 67 of the Information Technology Act, 2000 (IT Act) is often used against employees of digital businesses as it has provisions for imprisonment for three to five years. Recently, the managing director, who was neither the producer nor the show's director and was not credited in the episode, of a digital media streaming business was charged with multiple FIRs for publishing obscene material and hurting complainants' religious feelings under this Section.

For instance, in the Payments and Settlement Systems Act, 2007 (PSSA), Section 26 provides for imprisonment for as little as one month to as extreme as ten years, which was deemed an unnecessary criminalising provision. Such provisions do not have the desired deterrent effect as the businesses are able to continue their operations. On the contrary, these provisions create a business environment which is not conducive for growth, innovation and sometimes might lead to businesses withdrawing from the country.

Recommendation

- Adoption of a Civil Liability Framework similar to the one for Intermediaries in Brazil: Under this framework, *the Marco Civil Da Internet of Brazil,* the intermediaries are subject to civil liabilities in place of criminal liabilities and that has created a better environment for digital businesses.
- Adoption of a liability shield for intermediaries against third party actions with regards to content: In addition to this, laws with imprisoning clauses must satisfy the test of necessity and proportionality.
- Repealing laws without adequate safeguards to protect the interest of citizens and Intermediaries.

Regulatory Uncertainty

Key Findings

This Chapter underscores the reasons that cause regulatory uncertainty, including lack of regulatory framework, excessive delay in enactment of regulations, arbitrary approach of regulators, sub-optimal or ambiguous design, incorrect interpretation and failure in effective and efficient implementation. This impacts investment business decisions. For instance, in the cryptocurrency sector, due to the regulatory uncertainty, reportedly, companies have to restructure their strategies. In November, 2021, with the listing of the Crypto Bill, 2021, many crypto exchanges suspended ads for a couple of weeks and restarted when the government clarified that the bill would seek to not ban but regulate crypto-assets.

Recommendations

- Formulating an overarching principles-based regulatory framework, inspiration for which may be taken from the United Kingdom Government's Digital Charter: This will help in guiding regulatory actions, giving digital businesses a semblance of proposed regulations. Further, adopting a holistic government approach which facilitates regulatory collaboration is required to avoid regulatory turf wars, which creates regulatory uncertainty.

- Effectively engaging the Parliament, where relevant standing committees review regulatory actions of regulators, will help establish accountability of regulatory actions. Further, creating a mechanism for informal guidance which digital businesses can seek from regulators can also reduce regulatory uncertainty.

Unnecessary Compliance

Key Findings

In this paper, we use elements from the globally acclaimed **regulatory guillotine framework** and expand upon the core principles of 'is it legal', 'is it necessary', 'is it business friendly.' With the use of case studies and contemporary examples, the use of regulations under the Information Technology Act, 2000, Payments and Systems Act 2008 and Consumer Protection Act, 2019 and the E-Commerce Rules, 2020 thereunder, amongst others, have been looked at. For instance, the recent CERT-In directions under CERT Rules 2013 have multiple new compliances which are unnecessary. The impact of unnecessary compliances on smaller businesses and start-ups has been disruptive and thus the burden needs to be lessened.

Recommendations

- To Simplify, Amend or Repeal unnecessary compliances by making a government-led central repository of compliances for specifically digital businesses as a subset of the larger compliance portal: Further, the use of technology similar to Regulation Technology (RegTech) to ease compliances and their costs is also recommended.
- Institutionalising Regulatory Impact Assessment (RIA) for lawmaking process and for using the regulatory guillotine framework for existing compliances. Also, the use of the One In One Out (OIOO) concept where each time a new compliance is introduced, that compliance should be able to replace at least one existing compliances not only in number but more so in the cost imposed by said compliance.

Inadequate Digital Infrastructure

Key Findings

The discussion paper highlights layers of digital infrastructure and related challenges such as lack of digital connectivity, Internet shutdown, lack of data centres, lack of digital literacy, culture, trust, cyberthreat, India Stack, Open National Digital Ecosystem and Open National Digital Commerce. This adds the extra financial burden, limiting the scope of the expansion and increasing the challenges in operationalisation of the digital businesses. For instance, access to digital connectivity and shutdown of the Internet impacts smaller digital businesses disproportionately, sometimes they have to shut down their businesses. Along with this, the paper establishes that EoDDB, digital infrastructure and EoL are interdependent.

Recommendations

- Enhancing digital connectivity: For this, a framework of meaningful connectivity should be used which goes beyond access to the Internet. Instead of shutting down the Internet, specific websites and/or applications should be taken down on the basis of necessity and proportionality.
- Existing cybersecurity mechanisms need to be integrated and institutionalised which will enable robust and coordinated approach in strategically tackling cyberthreat. Also, India should develop digital public infrastructure through a transparent and participatory process to minimise its unforeseen implications such as exclusion and inaccessibility.

Restriction on Cross-Border Data Flow

Key Findings

Legitimate anxieties over surveillance, security and economic inequality are justifying governmental measures of restriction on cross-border data flow. The issue stemming from data localisation mandates poses critical concern to the future of international trade, doing digital businesses, addressing fraud

and countering cyber security threats globally due to siloed data-driven digital economy, as it erects borders in cyberspace. This will hamper the growing realisation of a globally connected digital economy which is the fundamental spirit of the Internet – free, decentralised and open network.

Recommendations

- Data localisation needs to define the objectives and process to achieve the intended aims clearly and periodically analyse their impact before taking any decisions: In addition to this, India should consider good practices such as APEC and steer in developing guiding principles for allowing the processing of data beyond national borders.
- Data protection mandates should take a more nuanced approach in safeguarding the privacy of individuals, sovereignty, international trade and doing digital businesses. This must ensure minimisation of unintended consequences by conducting surveys about the firm-level impact of data localisation.

The EoDDB study is an attempt to provoke further discussions and reforms in order to ensure innovations, competitiveness and welfare of the consumers. This study on EoDDB is just a beginning and many more in-depth works are required on each identified factor, including developing EoDDB ranking. This will be necessary to realise India's dream of becoming a global leader in the digital economy by making governance optimal and protecting the interests of all stakeholders.

2 CHAPTER Introduction and Scope

Introduction

Background

As the world evolves with technological transformations, any economy's long-term growth will be dependent on technological progress.[1] Abundance of daily online connections and transactions between consumers and businesses make networked architecture the backbone of the digital economy. This backbone is changing the conventional notions about how businesses are structured, how they interact and how consumers obtain services, information and goods.[2]

The COVID-19 pandemic has accelerated this change, as many companies have upgraded their infrastructure with substantial investments to survive and sustain themselves.[3] Similarly, many consumers went online for the first time, opening a significant window of opportunity for businesses to improve services, invest, innovate, compete and grow. During this transition, Satya Nadella, Microsoft's Chief Executive Officer (CEO), remarked that the world had seen a two-year digital transformation in two months.[4]

As per the report[5] of the Ministry of Electronics and Information Technology (MeitY), India aims to create an economic value of US$1tn from its digital economy by 2025. The report stated that the existing and continuously evolving digital ecosystem could generate US$200bn annually,[6] which is about 8.2 percent of India's Gross Value Added (GVA) in 2020.[7] However, digital businesses have been facing complex challenges in terms of regulatory and policy changes.

Increasing Recognition for Ease of Doing Digital Business

Globally, digital businesses are seen as entities requiring specialised policy and regulatory interventions compared to traditional businesses. The World Bank, in collaboration with the International Telecommunication Union (ITU), has published the Digital Regulation Handbook, which provides detailed guidance and case studies of best practices in regulating the digital economy.[8] According to the ITU, the impact of digital regulation needs assessment as the digital markets are increasingly becoming powerful drivers of social and economic growth.[9] Policies that are practical, agile and scalable would have a multiplier effect on digital markets and economies which translates to ease of living for people.[10]

Society and the economy are rapidly changing as traditional business models are being digitally shaped and industries turned upside down. The public and private sectors celebrate digital innovation, efficiency and flexibility, but potential risks also lie ahead.[11] It is important to note that, for a digital transformation, digital businesses have played a key role. Thus, it is also pertinent to facilitate their growth while maintaining consumer protection.

Tufts University Report 2019

The World Bank's Ease of Doing Business (EoDB) rankings (now discontinued)[12] do not explicitly differentiate between digital and traditional businesses. To fill this void and ascertain the conduciveness of a country for technology-based companies, Tufts University[13] (TU) released a ranking[14] on the Ease of Doing Digital Business (EoDDB) in 2019.

The TU Report relied on three foundational factors; namely, World Bank's Doing Business rankings, Digital and Analog Foundations (perceived indicators descriptive of foundations—i.e., the Demand, Supply, Institutions, and Innovation conditions— essential for all digital platforms), and Data Accessibility (the measure of free flow of data as well as government openness to sharing anonymised data publicly and policies in place to safeguard user privacy). x

In these EoDDB rankings for 42 countries, India was placed at the 38th position because of frequent policy reversals like the E-commerce Rules, 2019[15] and the lack of appropriate physical and digital infrastructure for digital businesses. While the sample size of countries in the EoDDB rankings appears to be small, given India's rank, attention is warranted to investigate various factors that exacerbate the unease of doing digital business in India.

Need for a Study on EoDDB in India

EoDB Reforms Undertaken in India

Over the years, the Government of India (GoI) has taken various measures to improve its position in the World Bank's EoDB rankings (now discontinued). India's ranking grew by 79 positions in five years (2014-2019). As part of reforms, GoI introduced the Insolvency and Bankruptcy Code, 2016,[16] and the Central Goods and Services Tax Act, 2017 (GST),[17] along with decriminalising various provisions in the Companies Act, 2013, and the Limited Liability Partnership Act, 2008 (LLP Act).[18]

The Companies Law Committee report[19] encouraged the introduction and use of the In-house Adjudication Mechanism Framework[20] (IAM framework) provided under Section 454 of the Companies Act, 2013, instead of being treated as criminal offences.

Further, the GoI has set a list of reforms for the Business Reform Action Plan[21] assessment to create a ranking system of states for enabling EoDB, which led to amendments in the Arbitration and Conciliation Act, 1996,[22] along with a reduction in corporate tax and labour reforms in over 20 Indian states like Gujarat, Andhra Pradesh, Tripura, Rajasthan, etc. This has also contributed to improving EoDB in India.[23]

Recently, the Indian Parliament abolished a retrospective tax law[24] and the Supreme Court upheld the sanctity of arbitration written into contracts. These measures have benefited the environment and confidence in EoDB in India.[25] In addition to the above, the Department of Telecom (DoT) also introduced numerous procedural and structural reforms[26] to facilitate competition and growth in the telecom sector, the telecom companies have been burdened due to financial liabilities arising from judicial disputes.[27]

Developments since TU Report 2019

Since the TU Report was released in November 2019, the world has gone through a platonic shift due to the COVID-19 pandemic and the uprising of digital technology. After the pandemic, surveys showed that leaps amounting to five years were made in eight weeks in the digital adoption of consumers and businesses.[28]

Further, the World Bank released a final paper on Doing Business[29] in 2021, which gave five indicators for digital businesses, including connectivity[30], data privacy and security[31], logistics[32], payments[33] and digital market regulations.[34] These indicators measure laws, regulations and policies from the lens of digital businesses and they cover multiple issues across different global economies and are relevant to this study.

While the digital adoption and transformation have been significant, the regulatory and policy changes and their implementation have not been optimum for technological innovations and changes.[35] The TU Report has also highlighted that nations are choosing to introduce regulations that impede new and existing digital businesses instead of creating an ecosystem where digital platforms become engines of livelihood and inclusion in the global marketplace.[36]

The EoDB reforms undertaken by GoI have been useful. Similar contours must be traced while promoting EoDDB as digital businesses are unique and different and cannot be covered entirely by traditional business rules and regulations. The government is responsible for policies and regulations that provide an environment that can enable technological change.[37] A lack of optimal regulations may

lead to unintended consequences for digital businesses. Further, inadequate regulations also undermine the opportunities that digitisation provides to an economy.[38]

Thus, this further necessitates evaluating factors that facilitate or hinder EoDDB in India. This study holds significance as EoDDB finds itself in accordance with the many initiatives of the GoI such as EoDB (highlighted below), Ease of Living (EoL), Digital India, and Start-up India, *and Atmanirbhar Bharat*, among others. These initiatives indicate the government's intentions to have a digital-first economy.[39]

Today, a technological edge can help in a country's socio-economic progress and indigenous technology development is a proven way of staying self-reliant and resilient. The state has a role in facilitating it by enabling policies, arranging investments and incentivising stakeholders to perform their roles.[40] It will, thus, aid in identifying consistency between the government's initiatives on facilitating business within the digital ecosystem.

Scope of the Study

What Constitutes a Digital Business?

The meaning of digital business varies, without any globally accepted definition. The TU Report defines digital businesses as having a digital platform core to their business models. According to Wall et al. (2007), the definition of the digital business largely depends upon the user and context.[41] As per Gartner, a digital business is the creation of new business designs by blurring the digital and physical worlds.[42]

Digital businesses create a competitive edge based on unique digital and physical resource combinations. They use technology as an advantage in their internal and external operations.[43] They use strategic options for transformation and have significant use of digital technologies to devise new value propositions for consumers.[44] They apply digital technology to reinvent business models and transform a company's products and consumer experiences—innovating products that create new value and connecting people with things, insights and experiences.[45] They use technology to create new value in business models, consumer experiences and the internal capabilities that support their core operations. The term includes both digital-only brands and traditional players that are transforming their businesses with digital technologies.[46]

All businesses may seem to possess some digital component[47] such as using online tools for operations, finances, management, etc. Still, digital businesses are unique as their business model primarily relies on digital technologies.[48] The factors that make digital businesses distinctive may include:

- Distinctive growth and contraction due to the uniqueness of the digital ecosystem
- Market resistance and competition issues are different
- Nuanced regulatory challenges
- Different preferences and priorities provided by the government
- Rules of data mobility, user privacy, etc. can affect EoDDB

Digital Business and Scope of this Study

The definitions mentioned above vary in nature; thus, creating a definition of digital business to limit this study's scope is necessary. Hence, this study defines digital businesses as businesses that use digital technology as a core[49] to their business. The core of all businesses might vary; however, in all viewpoints, the most critical part of the business is digital. These businesses may not generate content, products or services. Still, they reinvent the business models to use technology to enhance the consumer experience directly or indirectly and transform the ways any business or activity is normally conducted.

It is acknowledged that during the pandemic, many businesses moved towards digitising some aspects of their operations. Some businesses were unsuccessful in the required digital transition and remained on the fringes of the digital economy. These businesses are outside the scope of this study due to the vastness of the number and limited capacity to reach them.

Which Factors Impact EoDB?

Before illustrating the factors that may be affecting EoDDB, it is important to highlight the various factors which impact EoDB. This will facilitate a directional understanding of the factors which may impact EoDDB.

According to the World Bank Doing Business Report[50] 2005, EoDB is directly related to a country's regulatory environment and its conduciveness to business operations. The theory of economic regulations[51] suggests that variations in economic regulations on entry, exit, product, price and quantity or market structure can affect investment decisions.

Regulations often miss their goals because of factors like government overreach and one inefficiency being replaced by another. Governments, sometimes by intent or ignorance, adopt or maintain regulation that burdens entrepreneurs, leading to foreign investors avoiding economies that use regulation to manipulate the private sector.[52] A country's regulations could impede or facilitate foreign direct investments (FDI).[53]

While market regulations such as pricing can impact multinational corporations' (MNCs) profitability, a country's contract enforcement and the rule of law also impact MNCs' conduct and profitability in the marketplace, as well as the decision to enter the country in the first place.[54] The effect that a country's business regulatory environment has on the amount of FDI it attracts establishes a direct correlation between ease in compliance requirements and improved foreign investments.[55]

In the context of EoDB, the factors that impact businesses relate to setting up, winding up, operations and dispute resolution procedures. The 12 indicators[56] laid down in the '2020 Doing Business report' (now discontinued) by World Bank[57] can also be categorised into two large sections: ***Regulations*** and ***Infrastructure***.

Which Factors Impact EoDDB in India?

For the scope of the study, contemporary policies and practices specifically directed toward digital businesses are studied. This does not include policies applicable to both traditional and digital businesses. In no way does this conclude that they are less important or impactful on EoDDB. However, in the interest of time and capacity, they are kept outside the scope of this study.

Compared to EoDB reforms, the regulatory framework and reforms for digital businesses in India are not optimum for facilitating EoDDB. As the discourse on evaluating EoDDB is sparse, linkages can be made with traditional businesses to understand how regulatory and other factors impact the doing business ecosystem. Although the distinctions between traditional and digital businesses are unique, some regulatory requirements may be common for both. In contrast, the policy ecosystem and the associated factors impacting digital businesses could be varied.

In the context of this study, the factors that might impact EoDDB can be adjudged under two large umbrellas as described in the World Bank EoDB study, which are **(i) regulations** that govern business practices through rules, procedures and compliances and **(ii) infrastructure** which leads to ease of doing any business such as connectivity, digital literacy amongst others. Under these two umbrellas, various factors impact EoDDB and need to be evaluated. They are highlighted below:

(i) Criminalising Provisions: Decriminalisation of offences stimulates foreign investments, encourages formalisation of small businesses, and contributes to inclusive growth, which are vital for a healthy economic recovery following the COVID-19 pandemic.[58] According to a consultation paper of the Ministry of Finance, GoI, the risk of imprisonment for actions or omission without malafide intention hurts domestic and foreign investments.[59]

In 2018, it was predicted that the proposed amendments to decriminalise the Companies Act and other allied legislation would positively impact EoDB in India.[60] While GoI has decriminalised provisions directly relating to traditional businesses to facilitate EoDB, it has been noticed that this initiative of GoI is not positively contributing to EoDDB. This is evidenced by current laws directed at digital entities which contain criminalising provisions. How criminalising provisions impact EoDDB needs to be studied.

(ii) **Regulatory Uncertainty:** Policies and regulations can lead to uncertainty for businesses due to ambiguity in their framing. arbitrary actions of regulators also impact business decisions. Further, uncertainty in legal processes and lengthy litigation resolutions in court can also negatively impact EoDB.[61] How regulatory uncertainty has impacted EoDDB, and the digital economy remains to be examined.

(iii) **Unnecessary Compliances:** It has been observed that small businesses have to incur disproportionate costs of regulations, as a result of which they remain stunted. Compliances which may have been brought for large digital businesses certainly impose avoidable costs on smaller digital businesses and start-ups in India. Such policies and practices' impact on digital businesses must be explored.

(iv) **Restrictions on Cross-Border Data Flow:** Several existing and proposed policies and regulations mandate data localisation in India and restrict cross-border data flows. Literature shows that such restrictions negatively impact EoDDB in India. However, in light of the recent developments, a nuanced evaluation of the current status contains merit.

(v) **Inadequate Digital Infrastructure:** Inadequate digital infrastructure may impact the growth of digital businesses. Digital Infrastructure is one integrated system with two main categories: hard (physical) and soft (non-physical).[62] The hard category has two components, Connectivity and Transportation and Storage and Processing and the soft category comprises two components: Services & Applications and Terminals and Devices.[63] The issues of inadequate internet access, low levels of digital literacy, logistics for data storage and cultural and language barriers, amongst others, are some of these sub-factors in India's context. These issues warrant further attention.

These developments are emerging and evolving and, thus, would be further studied to understand the applicability of regulatory principles/frameworks for digital economy/businesses, including illustrating recommendations for an optimal regulatory approach in India towards fostering EoDDB and, hence, EoL.

Thus, under the **regulations** umbrella of this study, aspects such as **(i) criminalising provisions, (ii) regulatory uncertainty, (iii) unnecessary compliances** and **(iv) restrictions on cross-border data flow** will be covered. In addition, the **infrastructure** umbrella will cover the issue of **(v) inadequate digital infrastructure** covering the aspects of logistics, connectivity and public digital infrastructure, etc.

Endnotes

1 Martin Weitzman, Economist at Harvard, *available at* https://contxto.com/en/soapbox/technology-sustainable-society-5-0/

2 'What is the digital economy? Unicorns, transformation and the internet of things'; Deloitte, *available at* https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

3 Leaving No One Behind: Fostering an Inclusive E-commerce Ecosystem in India, CUTS CCIER, *available at* https://cuts-ccier.org/pdf/whitepaper-fostering_an_inclusive_e-commerce_ecosystem_in_india.pdf

4 Sparto, Jared, '2 years of digital transformation in 2 months', April 30, 2020, Microsoft, *available at* https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

5 'India's trillion-dollar digital opportunity,' Ministry of Electronics and Information Technology, *available at* https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

6 *Ibid*

7 Gross value added at basic prices (GVA) (current US$) India, *available at* https://data.worldbank.org/indicator/NY.GDP.FCST.CD?end=2020&locations=IN&start=2020&view=bar

[8] 'Digital Regulation Handbook; World Bank and International Telecommunication Union, *available at* https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/DigiReg20.aspx

[9] 'Digital regulation: 7 ways to move the cursor', ITU, *available at* https://www.itu.int/en/myitu/News/2021/02/15/10/44/Digital-regulation-7-ways-to-move-the-cursor

[10] *Ibid*.

[11] 'Could Regulation put the Brakes on the Digital Economy?', Bearing Point, *available at* https://www.bearingpoint.com/en/our-success/insights/could-regulation-put-the-brakes-on-the-digital-economy/

[12] The EoDB rankings of the World Bank have been discontinued as of September 16, 2021, *available at* https://www.worldbank.org/en/news/statement/2021/09/16/world-bank-group-to-discontinue-doing-business-report

[13] Chakravorty, Bhaskar et.al, 'Ease of Doing Digital Business 2019', November 2019, The Fletcher School, Tufts University, *available at* https://sites.tufts.edu/digitalplanet/files/2020/03/Ease-of-Doing-Digital-Business-2019_2020.pdf

[14] The ranking uses various parameters such as ease of starting, running and folding an enterprise (EoDB rankings) and ease of data accessibility, mobility, user sophistication, digital infrastructure, etc. The study has used variables and data from many sources, including the World Bank EoDB rankings and data used for the same.

[15] Findlay, Stephanie; Kazmin, Amy, 'India's e-commerce law forces Amazon and Flipkart to pull products', financial times, *available at* https://www.ft.com/content/29a96ff6-2615-11e9-8ce6-5db4543da632.

[16] The Insolvency and Bankruptcy Code, 2016, *available at* https://www.mca.gov.in/Ministry/pdf/TheInsolvencyandBankruptcyofIndia.pdf

[17] Central Goods and Services Tax Act, 2017, *available at* https://cbic-gst.gov.in/CGST-bill-e.html. Further research on the benefits of GST is warranted.

[18] Chitravanshi Ruchika, 'Govt decriminalises Companies Act to promote greater ease of doing business', September 21, 2020, Business Standard, *available at* https://www.business-standard.com/article/economy-policy/govt-decriminalises-companies-act-to-promote-greater-ease-of-doing-business-120092000398_1.html

[19] 'Report of The Companies Law Committee', February 2016, Ministry of Corporate Affairs, Government of India, *available at* https://www.mca.gov.in/Ministry/pdf/Report_Companies_Law_Committee_01022016.pdf

[20] The In-House Adjudication Mechanism under Section 454 of the Act (the "IAM Framework") was one of the key amendments introduced by the Companies Amendment Act 2019 to alter how certain compoundable offences under the Act are dealt with. The IAM Framework substituted the process of appeal and adjudication before the National Company Law Tribunal ("NCLT") with an online platform administered by the MCA about certain identified offences.

[21] State Business Reform Action Plan -2019 Implementation Guide for States/UTs, 2019, Department for Promotion of Industry and Internal Trade, *available at* https://dpiit.gov.in/sites/default/files/Implementation_Guide_2019_dated_04022019.pdf

[22] The Arbitration and Conciliation (Amendment) Act, 2021 enables automatic stay on awards in certain cases where the court has prima facie evidence that the contract of the award was affected by fraud and corruption. Similarly, the amendment omits Eight Schedule from the principal Act, which specifies the regulations, qualifications, experience and norms for accreditation of arbitrators.

[23] '15 States complete ease of doing business reforms', February 2021, Ministry of Finance, *available at* https://pib.gov.in/PressReleasePage.aspx?PRID=1698600

[24] The Taxation Laws (Amendment) Bill, 2021, offers to drop retrospective tax claims against companies on deals before March 2012 that involve the indirect transfer of Indian assets on fulfilment of conditions such as withdrawal of pending litigation and assurance that no claim for damages would be filed.

[25] Chaturvedi Arpan, 'Amazon Vs Future Retail: Supreme Court Upholds Validity Of Emergency Arbitrator', August 2021, Bloomberg Quint, *available at* https://www.bloombergquint.com/law-and-policy/amazon-vs-future-retail-supreme-court-upholds-validity-of-emergency-arbitrator

[26] Some reforms include a 4-year moratorium period on the Adjusted Gross Revenue (AGR) and spectrum dues with an option to convert interest on penalty dues into equity; AGR definition excludes non-telecom revenues; 100% FDI under automatic route permitted; among others.

[27] 'DoT amends licence norms to ease the financial burden on telecom sector', October 2021, LiveMint, *available at* https://www.livemint.com/industry/telecom/dot-amends-licence-norms-to-ease-financial-burden-on-telecom-sector-11633169281247.html

[28] Baig, Aamer, et. al, 'The COVID-19 recovery will be digital: A plan for the first 90 days', May 14, 2020, McKinsey Digital, *available at* https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days

[29] 'Doing Business: External Panel Review Final Report', September 2021, World Bank, *available at* https://www.worldbank.org/content/dam/doingBusiness/pdf/db-2021/Final-Report-EPR-Doing-Business.pdf

[30] **Connectivity Indicator** measures the good regulatory practices that promote universal access to broadband, efficient spectrum management, and accessible and safe domain name registration.

[31] **Data Privacy and Security Indicator** is a measurement of the good regulatory practices that promote the secure and ethical collection and dissemination of personal data, guaranteeing individual data subject rights, and the laws and regulations that encourage the free movement of data across borders.

[32] **Logistics Indicator** measures the costs associated with the small parcel trade, customs duties, value-added taxes (VAT) and goods and services taxes (GST).

[33] **Payments Indicator** is a measurement of the online payment cycle, explicitly observing the regulations that affect the online payments architecture, including the system's security, the protection of consumers' rights and data, and the quality and speed of online payment services.

[34] **Digital Market Regulations Indicator** measures the laws and regulations that promote digital transactions, transparent rules for sellers and consumers, and the safety and security of the digital marketplace.

[35] 'Rapid technological change threatens to outpace public policy', May 2018, UNCTAD, *available at* https://unctad.org/news/rapid-technological-change-threatens-outpace-public-policy

[36] Tufts University Report 2019 classified digital businesses into four categories: e-commerce, digital media, sharing economy, and online freelance.

[37] 'Technology and Innovation Report 2021', eISBN: 978-92-1-005658-8, UNCTAD, *available at* https://unctad.org/system/files/official-document/tir2020_en.pdf

[38] Digital Transformation Initiative, 'Unlocking $100 Trillion for Business and Society from Digital Transformation' May 2018, World Economic Forum, *available at* http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-executive-summary-20180510.pdf

[39] Holla, Nisha, 'The Role of the State in Facilitating an India-First Technological Imperative', Issue No. 344, January 2022, Observer Research Foundation, *available at* https://www.orfonline.org/wp-content/uploads/2022/01/ORF_OccasionalPaper_344_IndiaFirstTechImperative.pdf

[40] *Ibid*.

[41] B. Wall, H. Jagdev and J. Browne, 'A review of eBusiness and digital business—applications, models and trends', Production Planning & Control, Vol. 18, No. 3, April 2007, 239–26, *available at* https://www.researchgate.net/publication/245310273_A_review_of_eBusiness_and_digital_business-applications_models_and_trends

[42] Digital Business, Gartner Glossary, *available at* https://www.gartner.com/en/information-technology/glossary/digitalbusiness&sa=D&source=editors&ust=1632739090311000&usg=AOvVaw3QJhFNngw7INnZl7Cf3VjI

[43] 'What is Digital Business', Komprise, *available at* https://www.komprise.com/glossary_terms/digital-business/

[44] Slywotzky, Adrian, et al., 'Digital Business', February 2022, The Economic Times, *available at* https://economictimes.indiatimes.com/opinion/et-citings/digital-business/articleshow/85664468.cms

[45] What is Digital Business, Cognizant, *available at* https://www.cognizant.com/us/en/glossary/digital-business

[46] What is Digital Business, Liferay, *available at* https://www.liferay.com/resources/l/digital-business

[47] All businesses in the present day and age use other digital components, such as Tally, smartphone, and Google account for storing contacts.

[48] Tufts University Report, 2019

[49] Core means an essential part of something as defined by the Macmillan's dictionary *available at* https://www.macmillandictionary.com/dictionary/british/core_1

[50] 'Doing Business in 2006: Creating Jobs', 2005, World Bank & International Finance Corporation, ISBN 0-8213-5749-2, *available at* https://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB05-FullReport.pdf

[51] Gary S. Becker, 'A Theory of Competition Among Pressure Groups for Political Influence', The Quarterly Journal of Economics, Volume 98, Issue 3, August 1983, Pages 371–400, *available at* https://doi.org/10.2307/1886017

[52] 'Doing Business 2020', 2020, World Bank, *available at* https://openknowledge.worldbank.org/bitstream/handle/10986/32436/9781464814402.pdf

[53] A foreign direct investment (FDI) is a purchase of an interest in a company by a company or an investor located outside its borders. Generally, the term is used to describe a business decision to acquire a substantial stake in a foreign business or buy it outright to expand its operations to a new region. It is not usually used to describe a stock investment in a foreign company.

[54] Contractor Farok J., Dangol Ramesh, uruzzaman N., Raghunath S., 'How do country regulations and business environment impact foreign direct investment (FDI) inflows?', April 2020, International Business Review, *available at* https://www.sciencedirect.com/science/article/abs/pii/S0969593118305997

[55] Corcoran Adrian, and Robert Gillanders. "Foreign Direct Investment and the Ease of Doing Business.", 2015, Review of World Economics, *available at* https://ideas.repec.org/a/spr/weltar/v151y2015i1p103-126.html

[56] 'Doing Business 2020', 2020, World Bank, *available at* https://openknowledge.worldbank.org/bitstream/handle/10986/32436/9781464814402.pdf

[57] *Ibid*.

[58] 'Decriminalisation of Companies Act: Decoding the COVID economic relief', July 2020, *available at* https://economictimes.indiatimes.com/small-biz/legal/decriminalisation-of-companies-act-decoding-the-covid-economic-relief/articleshow/77235232.cms

[59] 'Decriminalisation of Minor Offences For Improving Business Sentiment And Unclogging Court Processes', June 2020, Department of Economic Affairs, Ministry of Finance, *available at* https://dea.gov.in/sites/default/files/consultation%20paper%20decriminalisation_0.pdf

[60] Lai K., 'New bill could impact the ease of doing business in India', 2018, International Financial Law Review, *available at* https://www.proquest.com/scholarly-journals/new-bill-could-impact-ease-doing-business-india/docview/1993915971/se-2?accountid=13598

[61] *Ibid*.

[62] 'Digital Infrastructure Sector Strategy AIIB's Role in the Growth of the Digital Economy of the 21st Century', June 2020, Asia Infrastructure Investment Bank, *available at* https://www.aiib.org/en/policies-strategies/operational-policies/digital-infrastructure-strategy/.content/_download/AIIB-Digital-Strategy.pdf

[63] 'Digital Infrastructure Sector Analysis Market analysis and technical studies', January, 2020, Asia Infrastructure Investment Bank, *available at* https://www.aiib.org/en/policies-strategies/operational-policies/digital-infrastructure-strategy/.content/_download/Full-DISA-Report_final-with-Appendix-2020-01-10.pdf

3 CHAPTER Research Design and Methodology

1. Study Rationale

1.1 Research Objectives

Based upon the literature review and gaps identified in the previous Chapter, following are the research objectives of the study.

- To explore the impact of factors like criminalising provisions, regulatory uncertainty, unnecessary compliances, restrictions on cross-border data flows (CBDF) and inadequate digital infrastructure (collectively, identified factors) on EoDDB.
- To gain the perspective of digital businesses on how the identified factors impact their business and EoDDB, in general.
- To highlight possible strategies through which adverse impact on digital business can be minimised.

1.2 Research Questions

Based upon the research objectives, the study examines the below-mentioned research questions in the context of EoDDB in India.

- How do the identified factors impact EoDDB in India?
- To what extent do the identified factors impact EoDDB in India?
- What are the possible strategies to improve the EoDDB in India while optimally addressing the identified factors?

2. Research Design and Methodology

The posed research questions need to be filled through both secondary and primary research. Accordingly, the research for this study has been done using a mixed methodology approach, primarily relying upon (i) desk research, including analysis of relevant government policies, regulation, laws, bills, and consultation papers relating the identified factors and (ii) online as well as offline engagement with relevant stakeholders, particularly people working on the policy vertical of the digital business and experts working in the domain of technology policy and regulations. The research design consists of a three-staged process as outlined below.

2.1 Stage 1: Secondary Research

This stage involves an in-depth literature review of prevailing regulatory studies on regulatory frameworks regarding digital businesses in India and other jurisdictions. Under the study, five key important factors were identified which include criminal liability, regulatory uncertainty, unnecessary compliance burden, restrictions on cross-border data flow and inadequate digital infrastructure.

Through desk research, a critical analysis of policies on the subject is carried out to understand how the identified factors impact doing digital business in India. Based on this, an understanding of regulatory objectives, possible concerns, compliance challenges, adverse impact and approaches in other jurisdictions is developed. This has been captured in dedicated Chapters in the report on each of the identified factors.

2.2 Stage 2: Interaction with Digital Businesses

Along with a comprehensive secondary research on the identified factors, there is also a need to interact with digital businesses to understand their perspective, expectations, concerns, impact and challenges, with respect to the regulatory framework for digital business.

For this purpose, semi-structured interviews are utilised. The team, through various means including in-person and telephone interviews, interacted with 15 digital businesses from different sectors operating in India. These businesses were questioned about the identified factors. Findings of the interaction with digital business have been analysed and interpreted to ascertain key takeaways.

2.3 Stage 3: Interaction with Experts

The key findings were presented in a focus group discussion with experts, including representatives from government, think tanks, industry and law and consulting firms. The stakeholders' feedback and suggestions were sought on ways to meet regulatory objectives, without unnecessarily impacting EoDDB.

3. Structure of the Report

The goal of the outputs would be to emphasise the impact of identified factors on digital businesses. Accordingly, the key Chapters under this study are:

- Dedicated Chapters on the five identified factors impacting EoDDB. These Chapters have also been released as discussion papers for engaging with key stakeholders, including policymakers, bureaucrats, industry bodies, etc.
- A dedicated Chapter highlighting the findings from the interaction with digital businesses and focus group discussion with key stakeholders.

4
CHAPTER

Impact of Criminalising Provisions on Ease of Doing Digital Business in India

Neelanjana Sharma, Senior Research Associate, CUTS International

Overview

In the Ease of Doing Digital Business (EoDDB) Study course, the researchers have taken up a discussion paper series on various topics that impact Digital Businesses in India. This Paper will discuss the aim of India's Digital First Economy and the role of Digital Businesses in its realisation.

The paper will introduce the Ease of Doing Business (EoDB) reforms undertaken by the Government of India, emphasising decriminalisation of regulations to enhance EoDB. Further, it explains criminalising provisions and tries to decode them for digital businesses in India. While decoding the criminal provisions, the paper covers regulations containing the imprisonment provisions and their use in judicial cases. It also discusses Brazil's civil liability framework for intermediaries along with other best practices across some countries. In conclusion, the paper tries to elaborate upon the way forward while suggesting some recommendations for the future of criminal liability of digital businesses in India.

Introduction

India aims to be a digital-first economy and seeks to create an economic value of US$1tn from its digital economy by 2025, as per a report[1] by the Ministry of Electronics and Information Technology (MeitY). For the digital economy and businesses to flourish, a regulatory environment and ecosystem that enables such growth must be fostered, assisting India's EoDDB. One of the key aspects that impact businesses, traditional or digital, is the country's regulatory environment.

Over the past decade, India has made substantial progress towards EoDB reforms. One of the key steps taken was removing criminalising provisions from several regulations and laws, which encouraged innovation and increased the entrepreneurial spirit of the youth. However, this non-criminalising touch of the government remains aloof from the businesses that have digital at their core or which exist digitally alone and deal with consumers' data.

Rapid digitalisation has turned out to be a double-edged sword for the government. It has opened up the markets for innovation and has increased access to information, goods and services in India. However, it has also accelerated regulation development on a still young landscape. Regulations are not always of the nature to promote the EoDDB.

In this paper, the parallels between the regulatory intentions towards digital and traditional businesses from the lens of criminalising provisions and their usefulness are brought to light. This paper aims to initiate a discourse on the gap between traditional and digital businesses and their regulatory environment in India. With the acceptance and encouragement of EoDB, India should also cater to EoDDB to achieve its goal of a digital-first economy. This paper will attempt to reveal the hindrances caused by criminal penalties; later will decipher alternate mechanisms which can be used to avoid such hindrances while fulfilling the objectives of such provisions.

The rule of criminal liability stands upon the maxim 'actus non facit reum nisi mens sit rea means', which can be loosely translated into that the Act is not wrongful unless it is done with a wrongful state of mind.

The offences would be dealt with by the adjudication officer of the IAM Framework, who would be able to determine penalties through order, the appeal of which would lie with regional directors.

Criminal Liability of Businesses

The traditional starting point of criminalisation is the 'harm principle' where John Stuart Mill stated that the only purpose for which power can be rightly exercised over the members of a civilised society against their will is to prevent harm to others.[2] The number of laws targeted towards digital businesses are not infinite but more than those required.

Though the corporation is a separate legal entity and can therefore commit a crime, the criminality principle cannot be exercised in isolation from the principle of proportionality. The principle of proportionality states that there needs to be a reasonable nexus between the desired results and measures taken to reach that goal.[3]

Criminal penalties in business mean terms of imprisonment for certain actions. The existence of criminal provisions for procedural, structural or minor offences suggest that violation of rules and non-compliances are offences of serious nature that require imprisonment as part of the punishment. As the criminal offence accompanies mens rea (mental intention);[4] the applicability of such jurisprudence to digital businesses seems at variance from traditional businesses.

Also, criminal penalties of imprisonment need to be viewed on its usefulness and effectiveness. One of the criticisms faced by the opposition of imprisonment clauses is that the provisions are hardly ever used. However, if the provisions are not used, their necessity should be taken on merit as a useless law weakens the necessary law. The distinction between what is necessary and what is useless perpetuates fear and questions the lawmaker's intent, which ends up criminalising entrepreneurship and business entities.[5]

Decriminalisation under EoDB

Due to pandemic India's EoDB framework streamlining has been pushed to the forefront and follows three steps: rationalising, digitising and decriminalising.[6] One of the key aspects of those reforms has been decriminalising various technical and procedural provisions. After extensive analysis, more than three hundred low risk offences have been decriminalised.[7] Below mentioned are some of the laws which were altered to keep up with the EoDB provisions:

The Companies' Act, 2013

In light of the pandemic, companies faced difficulties in keeping up with the regulatory and procedural aspects of the Companies Act 2013. The Government of India (GoI) had decriminalised certain provisions that contained compoundable offences to adapt to the changes. This was done keeping in mind the EoDB and promoting foreign investment. This will also encourage young entrepreneurs to start their businesses in India instead of seeking foreign jurisdictions and markets.

The 23 offences of minor nature, such as non-compliance, were reclassified and moved to In-House Adjudication Mechanisms (IAM) Framework as they were the offences that could be dealt with objectively.

Other than 23 offences, seven offences capable of being dealt with using other laws were excluded from the Companies Act. Furthermore, 11 offences that were not of grave violation and compoundable were restricted to the imposition of fine only as they involved subjective determination. The Company Law Committee (CLC) had recommended the creation of alternate mechanisms to impose a sanction and that recommendation was accepted as is by the GoI.[8]

The Limited Liability Partnership Act, 2008 (LLP Act)

After the Companies Act, to make LLPs feel like an interesting and safe option and encourage EoDB, GOI had approved decriminalising 12 provisions out of the total 24 provisions that were penalising in nature.[9]

To decriminalise the offences two major steps have been taken. Firstly, there has been the reduction of penalties for several compoundable offences and some of the offences of minor nature have been moved to IAM Framework.

In furtherance of the offences being punishable with fines, the regional directors can compound those offences. The scope of the section has been broadened to include the process of compounding of offences by the regional directors.[10]

India has over two lakh LLPs and in the past financial year, there has been a 17 percent growth in the number of LLPs incorporated in India. The amendment boosted the inclination towards LLPs and contributed towards EoDB.

Other Miscellaneous Measures for Decriminalisation

The Department of Financial Services, Ministry of Finance had also initiated a process by inviting public comments to decriminalise minor offences under 19 acts and financial laws for improving business sentiment and unclogging court processes.[11]

In view of the measures of decriminalisation undertaken by the GOI have given the strength to single businesses such as brand retailers to ask for decriminalisation of *The Legal Meteorological Act, 2009.*[12] Under this Act, 23 provisions have imprisonment provisions for offences of compoundable and non-compoundable nature. The retail businesses representatives claimed that the Act is archaic and involves imprisonment as punishment for offences that might be caused due to an oversight. GoI will soon finalise decriminalisation of offences on similar grounds as was done under the companies act and the LLP act.

Decoding the Criminalising Provisions for Digital Businesses

The advent of digital technology in all businesses is evident and even traditional businesses have some digital component in them. Rapid digitalisation has opened markets of innovations and increased access to goods and services, but it has also created a burden on the young regulatory landscape of the country.

This is exactly what intermediary liability entails for service providers in India. As elaborated above, corporate law jurisprudence in India is moving away from criminal liabilities towards civil sanctions. However, in the past decade, multiple regulations have been formulated which directly impact digital businesses. A few proposed and existing laws paradoxically mandate provisions that impose certain criminal penalties on digital businesses.

Such laws and regulations hinder investment decisions and make it challenging to do digital business. They could also convey contradictory approaches to the GoI's aim and objective to enhance EoDB in India.

Intermediary liability means that the intermediary is held liable for everything his users do -Rebecca MacKinnon.

Under the IT Act, Section 2(w) defines an intermediary as any person who on behalf of another receives, stores, transmits, records and provides services in respect of this record. It includes service providers of network, telecom, internet, web-hosting, search engines, amongst others.

Information Technology Act, 2000 (IT Act) and Rules thereunder

Under the definition of intermediaries, thus, digital businesses, which are social media companies, search engines, digital payment service providers, amongst others, are included. Therefore, any provision applicable to an intermediary would apply to these digital businesses, including provisions containing imprisonment clauses.

IT Act provides safe harbour provisions where Section 79[13] protects social media intermediaries against legal action for any third-party information, data, or communication link made available or hosted by it. However, this protection only applies if the said intermediary does not initiate the transmission of the message in question, select the receiver of the transmitted message, and do not modify any information contained in the transmission.[14]

Section 79 and associated rules introduced to protect intermediaries for liability from user-generated content and ensure the internet continues to evolve as a "marketplace of ideas". But as intermediaries may not have sufficient legal competence or resources to deliberate on the legality of an expression, they may end up erring on the side of caution and takedown lawful expression.[15]

Below are the sections explained through the case laws about their use and misuse of imprisonment clauses despite the Section 79 provision of safe harbour.

Section 67

Section 67 of the IT Act often includes managing directors and employees of any digital business. The punishment provided under the section consists of fines and imprisonment ranging from three to five years. After the strike down of Section 66 A of the IT Act owing to its rampant abuse, Section 67 is being actively misused to file complaints of cyber defamation.[16]

The CEO of an E-commerce portal was arrested under Section 67 later allowed bail because of an obscene video placed on the website. The CEO had to prove his due diligence.[17] However, the case was registered only for the CEO in this matter. The persons who uploaded the objectionable material remained unidentified, thus making the CEO liable for third-party action.

Recently, the managing director of Alt Balaji (a digital media streaming business) was charged with multiple FIRs (Hyderabad, Madhya Pradesh (MP), Delhi) for publishing obscene material and hurting complainants' religious feelings. It is important to note that MP FIR was registered by name and did not include the business' name. The managing director was neither the producer nor the show's director and was not credited in the episode.[18]

The FIR of the Delhi and Hyderabad case was later dismissed due to a lack of evidence in the case.[19] However, the MP High Court refused to quash the case,[20] and accepted that it can be presumed that a managing director having no part in conceptualising, publishing, directing and producing would have known the contents of each episode. The onus of proving otherwise was shifted to the managing director for proving, by way of evidence, that she did not possess such knowledge. Though the managing director issued a public apology and the scene in question was deleted without it requiring a direction from court, the managing director had to move the Supreme Court for interim protection from arrest.[21]

Through this scenario, one thing that can be implied is, the persons who created the episodes, the users who paid for the subscription and watched the episodes faced no criminal charges, however, a managing director with no criminal intent faced multiple FIRs.

Section 69 and Rules Thereunder

Under Section 69 of the IT act, Intermediaries are required to provide technical assistance and facilities for providing or securing access, intercept, monitor or decrypt and provide information stored in computer resources.

Intermediary in contravention with Section 69 and rules thereunder is liable to be punished with imprisonment up to seven years.

The procedure for the interception, monitoring and decryption is provided for in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (2009 rules),[22] which are to be read with Section 69 (2) of the IT act. Under Rule 21 of the rules mentioned above, it is stated that intermediaries can be held liable for any action of their employees and can be made liable under any law for the time being in force.[23]

In a 2022 case,[24] The appellant had filed an RTI to seek statistical data about Section 69, which was denied. In this appeal, the appellant also presented as evidence the pleadings of five petitions (pending before the Supreme Court) which challenged the constitutional validity of part of section 69, Section 5(2)

of the Telegraph Act, 1885 and rule 4 of the rules made under Section 69 B on the grounds of legislation not satisfying the test of proportionality put forth by the right to privacy judgement by the Supreme Court.[25]

The court adjudicated that, materials are retained for more than the prescribed period due to an overlap exemption under the rules. There is no reason for not providing the information sought under the Right to Information Act, 2005. However, some guidelines were prescribed for the duration for which data can be retained under every order and rules.

In between the challenges on validity scope of rule-making power of the provisions, one thing that remains intact and untouched is an intermediary liability. In India, the approach followed for intermediary liability is vertical in design, wherein different liability regimes under various statutes apply to intermediaries.[26]

Section 85

Section 85 of the IT Act makes the director and every person who was in charge and responsible for the conduct of the business at the time of the contravention liable to be proceeded against and punished. The section provides for an exemption from this liability in case the person is able to prove his due diligence which was then used by the CEO of Bazee.Com.

In a Delhi High Court Case, where profile pictures of the petitioner were taken from social media websites and uploaded on pornographic websites, no claim was sought by the petitioner from the social media websites.[27] However, in another case, the social media companies were directed to remove any other material the plaintiff may report as objectionable.[28]

The exemption provided under Section 85 and Section 79, however, seems infructuous after the release of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[29] (Intermediary Rules, 2021)

The above-stated provisions are the most commonly used imprisoning provisions. However, there are other provisions with imprisonment clauses that have the potential to be misused. The same is provided below.

Section 67 C and Rules Thereunder

Section 67C of the IT act if an intermediary intentionally or knowingly fails to preserve or retain information for a prescribed duration, manner and format for central government, then such intermediary shall be liable to be punished with imprisonment up to *three years*. GOI released the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.[30] Though the rules do not contain any provisions for imprisonment, they do place a compliance burden on intermediaries.

Under these rules, Intermediaries, internet service providers, websites, apps like Facebook, WhatsApp and Gmail are required to collect and store data. Data retention laws can quickly become a 'legal' means of violating people's fundamental right to privacy without the necessary safeguards.[31]

In case of infringement of the rules and Section 67 C, without taking it on a case-to-case basis or keeping a scope of communication of inability to comply with the law, the first step undertaken is imprisonment. It needs to be reiterated for the whole of IT Act that though well-intentioned, one of the major gaps in the implementation of the IT Act is that it wades into criminal liability straightaway. The case is not always wilful illegality, wherein a crime may have been committed but may not be intentional. It is not necessary to convict when penalising can achieve the goal.[32]

A writ petition was filed inter alia against search engine operators including Google, Yahoo and Microsoft, to hold them liable for displaying advertisements or searches in violation of the Prenatal Sex Determination Act, and the Court imposed obligations to monitor the complaints and respond to complaints relating to the Act upon the search engines.

Section 69 A and Rules Thereunder

Under Section 69A of the IT Act, Intermediaries can be directed to block public access by way of direction under written orders. In case an intermediary fails to comply with the direction, they can be punished with imprisonment up to *seven years*. Even though the constitutional validity of Section 69A has already been examined by the Supreme Court,[33] where the court noted that the section has been narrowly drafted and provides safeguards. However, it appears that such safeguards are not followed in practice, thus, making intermediaries criminally liable in case of non-compliance.[34]

Under Section 69 A, the GOI had framed the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules)[35] to lay down the rules regarding blocking of information to the public under the information of technology act as some of the confidential information cannot be disclosed.[36]

The government used these rules and section 69A to restrict access to accounts, sites, and networks multiple times, such as Chinese App ban, Twitter accounts, and tweets from certain accounts withheld.[37]

Even though the Blocking Rules exist and so does section 69A, recently, the Indian Supreme Court has held search engines, liable, as intermediaries, for hosting advertisements and keywords relating to pre-natal sex determination.[38] Court ordered actions for content restriction are outside of any explicit statutory authority, even though similar outcomes may be achieved through existing legislation, such as the Blocking Rules.[39]

Section 69 B

Under Section 69B of the IT act, Intermediaries are required to provide technical assistance and facilities for monitoring and collecting traffic data or information through any computer resource. Intermediaries in the contravention are liable to be punished with imprisonment up to *three years*.

Though the provision in itself seems straightforward, the 2009 Rules are also in convergence with this. On a closer look, Section 69 B empowers the Central Government to authorise any government agency to monitor and collect traffic data or information through any computer resource for cyber security. This sets the stage for direct Internet and internet metadata surveillance, respectively.[40]

Metadata includes internet usage and telephone data, such as time and duration of telephone calls, IP addresses, IDs of senders and receivers of e-mails, log-in and log-off times for e-mail use, etc. Such data excludes the actual content of the e-mails or the messages. While governments argue that metadata does not reveal the individual's personal details, this is not true. An individual's entire internet history can be traced out using just the metadata.[41] This nature of surveillance is dangerous as India currently does not have any Surveillance Reforms in place to protect citizens' privacy.

Section 87 and the Intermediary Rules, 2021 Thereunder

The intermediaries that can be held criminally liable are employees of digital businesses in this case which are specifically employed for compliance and operational purposes, such as compliance officers, directors and nodal officers as was made clear under the Intermediary Rules, 2021.

Further, the Intermediary Rules, 2021, prescribe guidelines for due diligence and grievance redressal mechanism for intermediaries and code of ethics, procedure and safeguards for digital media. In doing so, the rules categorise intermediaries into two distinct categories. Firstly, social media intermediaries primarily enable online interaction between users, allowing them to create, upload, share, disseminate, modify or access information using the intermediary's services.[42]

Secondly, significant social media intermediaries have a number of registered users as notified by the central government, which was later clarified to be at 50 lakh users.[43] These intermediaries would mean businesses such as search engines, internet service providers (ISPs), digital platforms, etc.[44]

Under the Intermediary Rules, SSMIs are required to appoint a chief compliance officer (CCO)[45], a nodal contact officer[46] and a resident grievance officer[47], all must be residents of India. The chief compliance officer is responsible for ensuring compliance with the IT Act and Rules, and will be held liable in any proceedings in instances[48] of non-compliance with the IT Act and Intermediary Rules.[49] Similar penalising provisions for non-compliance by other intermediaries are given under Rule 7 of Intermediary Rules.

The appointment of CCO was not without its troubles. The businesses were sceptical about the liabilities attached to the role. Experts suggested that the CCO be responsible for all compliance requirements and non-compliance shall entail jail term. According to Rule 7, non-observance of Rules may take away of the protection of Section 79 of IT Act and non-observance shall be punishable under any law, including IPC (Indian Penal Code) where criminal charges can be determined and sentence for jail is also possible for the CCO as per Rule 4(1) (a).[50] Also, the Intermediary Rules, 2021 provide for the CCO to be a key managerial person of the company, which can be the CEO or the MD, Chief Financial Officer (CFO), Manager, company Secretary or Whole Time Director.[51] This not only takes away the freedom of the businesses but also comes under the light of over-regulation.

Recently, in a series of First Information Report (FIRs) filed against Twitter, one of the executives in a statement to media questioned if someone will take a job if it came with a caveat of going to jail for a third party's tweet. Similarly, in one of the FIRs filed against Twitter related to the company misrepresenting India by not showing Jammu & Kashmir and Ladakh as outside India, the Managing Director and Twitter India's head of News Partnerships were named in the FIR, even though neither was directly involved in the process of making the maps.[52] The impact of these FIRs on the business can be evaluated from the update that the Managing Director was moved outside India and later ended up quitting Twitter entirely.[53] The automatic attachment of criminal intent with the position of a compliance officer is not only disproportionate but also a deterrent to businesses.

Also, one of the challenges to intermediary protection has been the use of platforms in criminal activities.[54] MeitY has taken up the issue on two separate occasions with WhatsApp and has indicated that if the intermediary does not find a solution for the same, they're 'liable to be treated as abettors' and 'face consequent legal action', which can mean that intermediaries are prosecuted as abettors under the Indian Penal Code (IPC).[55]

Here, there is a lack of clarity on which provisions from the IPC may apply in case of non-compliance and thus, the number of years of imprisonment may be varied for different kinds of non-compliances. This does not find mention in the Intermediary Rules.

The MeitY, in October 2021, had issued FAQs on the Intermediary Rules, to provide clarity and explain the nuances of due diligence to be followed by intermediaries.[56] Further, according to media reports, GoI is also considering amendments to the IT Act to bring in new penalties, such as fines, for social media companies and individuals and retain some of the law's criminal provisions.[57]

These rules have overtaken the Intermediary Guidelines, 2011, against which a petition was filed by MouthShut.com seeking their quashing because they are violative of Article 12, 19 and 21 of the Constitution of India.[58] In the past 10 years, not much has changed except new and more ways have made their way into laws to make intermediaries liable and to violate fundamental rights using the means of regulations.

Payment and Settlement Systems Act, 2007 (PSSA)

The PSSA provides for regulation and supervision of payments systems in India. Section 26(1) of the PSSA prescribes penalties to those who operate without authorisation[59] from the Reserve Bank of India (RBI)[60]. The penalty of imprisonment from 1 month to 10 years has to be judged based on the severity of this punishment which is on two extremes. The penalty of 10 years under the IPC is prescribed for offences of heinous nature, and anything below seven years of imprisonment is considered a serious offence.[61]

Although the provision is technical and procedural, Section 26(1) prescribes a penalty of imprisonment ranging from as little as one month to as extreme as 10 years or fines or both.

Out of the few provisions of the IPC which have prescribed the 10-year imprisonment, one is the offence of Culpable Homicide not amounting to Murder[62] punishable under Section 304.[63] Even this provision has an addition of 'may extend to 10 years.' It can be deduced that offences under PSSA Act are considered as grave as section 299 of IPC and as frivolous as one-month imprisonment. This will create unnecessary fear in the businesses and the need for such provision thus should be examined on its merit by the regulators.

Also, previously, the Ministry of Finance had called for comments on decriminalisation of thirty-nine minor economic offences, including Section 26(1) and 26(4) of the PSSA to facilitate ease of doing business in India.[64]

The regulator had identified some principles which directly relate to reclassification of criminal offences to compoundable offences such that they would lead to the following results:

a. Decrease the burden on businesses and inspire condense amongst investors;
b. focus on economic growth, public interest and national security should remain paramount;
c. mens rea or criminal intent plays a vital role in the imposition of criminal liability. Therefore, it is critical to evaluate the nature of non-compliance i.e., fraud as compared to inadvertent omission; and
d. the habitual nature of non-compliance.[65]

However, nothing came out from the finance ministry's move as there were no further updates on this action.

Joint Parliamentary Committee's Report on Personal Data Protection Bill, 2019 and Draft Data Protection Bill, 2021 thereunder

In addition to the above regulations, the recent recommendations by the Joint Parliamentary Committee (JPC) on the Draft Data Protection Bill, 2021 (DP Bill, 2021), suggested that social media companies that are not intermediaries or do not act as intermediaries should be treated like publishers.[66] JPC's recommendation to term social media platforms is flawed on the grounds established in *Shreya Singhal Case*[67], which struck down Section 66A[68] of the IT Act on online free speech and intermediary liability.

Suppose social media companies are termed as publishers and made accountable for any content they hold. In that case, it takes away the safe harbour provisions brought in effect in the 2008 amendment of the IT Act after the Delhi High Court decision in *Avinash Bajaj Case*.[69] It is implied that social media companies will start to pre-screen the content uploaded by the users to keep themselves safe from any liability, which would curtail Article 19(a).[70]

This would give the power of censorship to private entities and take away the freedom of speech and expression outside the reasonable restriction of Article 19(2), which can be imposed only by the state as defined under Article 12 of the Constitution.[71] Though the law is still to be brought in effect, this implication brings liabilities both of fine and imprisonment, which print and online publishers are subjected to under various laws.

Section 83(1) of DP Bill, 2021 states that whoever, without the consent of data fiduciary or processor, knowingly or intentionally re-identifies the data is liable to be punished with imprisonment of up to *three years*. Along with this, Section 85 of DP Bill, 2021 states that any company found in contravention of the Act, person in charge of that part of businesses conduct can be made liable and punished accordingly. Though, DP Bill, 2021's Section 83's call for imprisonment is against the use of personal data, which is justified in the right to privacy.

However, Section 85 of the DP Bill, 2021 mirrors in intention with Section 85 of the IT Act and places unnecessary burden on private data fiduciaries as opposed to government and its agencies who can be given blanket exemption under Section 35 of the proposed bill. If the bill sees the light of the day without any changes, this section might be susceptible to misuse, and experts have not caught up on it yet.

Copyright Act, 1957

The copyright act went through some amendments in 2012. Under Section 69 of the Act, companies and their director, manager, secretary, or other company officers can be made liable for offences under the Act and punished accordingly unless they can prove their due diligence.[72]

In the digital age, content is free-flowing and the buttons of like, share and facility of the screenshot in all smartphones have changed the way content is circulated. The copyright act assigns liability on key persons of the company and allows exemption in case of due diligence; however, as the intent is difficult to prove and not always criminal, the misuse of the section is more likely than its fair use.

The businesses, though, enjoy protection under 52(1) (b) and (c) and Section 79 of the IT Act. However, courts' opinion is often different from the section's purpose. In a 2008 case, search engine Google was charged with Defamation for hosting a blog on its platform.[73] Google India had moved the High Court of Andhra Pradesh to dismiss the criminal charges against it because it enjoyed safe-harbour protection under Section 79 of the IT Act.[74] Google India failed to gain said protection as it did not take down the blog after information and now will face trial in the case.[75]

Intermediaries have been charged with copyright infringement in cases because by allowing viewership and sharing of pictures along with music, it has knowingly allowed for infringement and has become a party in the infringement.[76] The court adopted a similar point of view in the case of Kent RO Systems.[77]

There is a lack of clarity in the law concerning intermediaries, and it does not lay down the kind of content that is not permissible under the law of copyright. Interme diaries find themselves at a loss as to what action to take for any such content as they might be required to monitor, track, retain or delete any data as per the various laws in the country. As the intermediaries, to protect themselves from liability, have taken to censorship.[78]

Disproportionate action taken against digital businesses through Code of Criminal Procedure, 1973 (Cr.PC)

Section 91 of the Cr.PC allows the court to issue notices for presenting any document or file by means of summons. However, in a recent case, it has been observed that this provision is used by the law enforcement authorities to freeze accounts under the pretext of an investigation into a cheating case.[79]

Intermediary Liability Across Global Jurisdictions

In order to respond to new market players and businesses, governments need to develop clear, coherent rules to facilitate digital economic activities. It is fairly important for developing economies like India, which have not fully reaped the benefits of the digital evolution for economic growth.[80]

Making the employees personally criminally liable[81] may adversely affect the business sentiment of digital businesses, consequently leading to enterprises wanting to leave the country, adversely affecting investments, employment, and welfare of the digital economy. Governments worldwide increasingly pressurise the intermediaries to block their users' undesirable content to suppress dissent, hate speech, privacy violations, and the like. These pressures often surface in making intermediaries legally responsible for the actions of their users.[82]

Marco Civil Da Internet of Brazil: A Civil Liability Framework for Intermediaries

Brazil is the only country with a specialised intermediary liability regime designed for Internet access providers and Internet application providers. The "Marco Civil" establishes exemptions to providers' liability in relation to third-party content, and access providers are always exempt from liability for user content and behaviour.[83]

The model chosen by Brazil in adopting its civil framework for the internet (Marco Civil da Internet) can be seen as an inspiration for the definition of principles underlying such global mechanisms. The model has two distinguishing provisions:

a. The multistakeholder nature of the process that led to the definition of the existing legal framework; and
b. the aspiration to give a "constitutional" dimension to such a framework, by recognising some fundamental rights and principles as founding pillars of internet regulation.[84]

The Marco Civil is also known as "constitution for the internet" because it revolves the whole regulatory framework around a number of guarantees for civil liberties, such as the privacy and freedom of expression of users.[85]

Another distinction in the Brazilian framework is that it distinguishes the intermediaries into two main categories (1) content producers who are publishers of content and (2) infrastructure providers who are not expected to detect or remove potentially illegal material.

Article 18 addresses the liability of Internet connection providers' liability and grants an exception to those services regarding intermediary liability. It states that "the Internet connection provider shall not be subject to civil liability for content generated by third parties".

Article 19, which addresses Internet application providers (excluding connection providers) states that, "to ensure freedom of expression and to prevent censorship, an Internet application provider shall only be subject to civil liability for damages caused by virtue of content generated by third parties.

The law introduced a liability exemption for *Internet connection providers* and the application of the safe harbour doctrine for other *Internet application providers*.

If, after a specific court order, an intermediary does not take action, according to the framework and technical limits of its services and within the time-frame ordered, to make the infringing content unavailable." For a literal interpretation of the law, neither the responsibility exemption to ICPs nor the safe harbour doctrine to ISPs would apply to criminal liability.[86]

Similar to Global Taxation of Tech Giants,[87] there is a need for a global regime of intermediary liability. Brazil's law based upon civil liability can provide the three base pillars for the development of intermediary liability regimes:

a. To identify the "constitutional ground" upon which an intermediary liability regime should be founded, supported by several principles safeguarding fundamental rights while encouraging private enterprises.

b. To accept the necessity of having a multi-stakeholder drafting procedure to achieve consensus over basic intermediary liability principles. This procedure would expose the need for a differentiated intermediary liability regime, particularly, for copyright and "revenge porn", by defining specific exceptions to those principles.

c. To understand the unsuitability of a "one size fits all" approach and how differential treatment in intermediary liability legislation should be at the core of future intermediary liability discussions.[88]

Along with the civil liability framework of Brazil, there are several principle-based laws detailed below, which can be best practices to borrow for India's regulations.

Publisher Liability of Intermediaries

Australia was one of the first countries to pass online intermediary liability legislation in 1992. Decades later, in 2019, it passed an additional law. In early 2021, the Australian government had passed legislation to enact a news media bargaining code to " address bargaining power imbalances between Australian news media businesses and digital platforms, specifically Google and Facebook.[89]

In addition to the awareness shield under Article 3 of Japan's Provider Liability Limitation Act, Japan has also stated that when providers block content, they are not liable for "any loss incurred by" the user who posted the content, as long as providers meet one of two requirements. First, if they had "reasonable ground… to believe that the rights of others were infringed without due cause" by the content in question, they are not liable. Second, if they receive a takedown notice, they must ask the user who posted the content for consent to remove it—and if the user does not respond within seven days, they are also not liable.[90]

The United States of America, provides under the Digital Millennium Copyright Act (DMCA) that online services are not liable for their "good faith disabling of access to, or removal of, material or activity claimed to be infringing, … regardless of whether the material or activity is ultimately determined to be infringing."[91] Instead, any individual who files a takedown notice or counter-notice is liable if they "knowingly materially misrepresent" that either the content in question was infringing, or that it was not infringing and was mistakenly removed.[92]

Similar provisions find a place in the **South African** legislation. Similarly, under Chapter XI, Section 77 of South Africa's Electronic Communications and Transactions Act, websites are not liable for a wrongful takedown if they remove the content in response to a takedown notice. Rather, the individual who submitted the notice is liable for damages if they knowingly misrepresented the facts.[93]

Intermediary Liability for Third Party Actions

In Australia, similar to the Indian IT Act, Schedule 5, Clause 91 of Australia's Broadcasting Services Act 1992 states that websites and Internet service providers (ISPs) are not liable for third-party content under state or territory laws as long as they were "not aware of the nature" of the content.[94]

However, The Copyright Act 1968 creates a system of secondary liability, expressly providing that infringement occurs if a person authorises an infringing act. part V div 2AA of the Copyright Act protects 'service providers' from copyright infringement in certain circumstances. The Australian High Court confirmed that where the publisher of a message is a 'mere conduit', the publisher is not liable.[95]

The Copyright Act 1968 is the only legislation to expressly attribute liability to an e-commerce platform where that platform has authorised an infringing act. The Federal Court held that Redbubble (an e-commerce platform) had communicated the copyrighted work (primary infringement); and secondary infringement would be made out.[96] Thus implying that platform operators will only be liable where they have been found to authorise copyright infringement (that is, the platform operator has enabled others to infringe copyright).[97]

The United States of America offers a unique and interesting case, from both a legal and policy perspective, to study the governance landscape for online intermediaries. The Communications Decency Act's Section 230 prevents online intermediaries from being treated as the publisher of content from users of the intermediaries.[98] Section 230 covers defamation, invasion of privacy, tortious interference, civil liability for criminal law violations, and general negligence claims based on third-party content. Section 230 also contains a few major exceptions; notably, its liability shield does not apply to federal criminal law, state or federal sex trafficking law, or intellectual property law instead of India's list of exemptions on public order, national security, etc.

South Africa's Electronic Communications and Transactions Act, enacted two years after the EU's E-Commerce Directive, contains sections on mere conduit in a similar language. South Africa's law does not include awareness or "actual knowledge" provisions. However, it does state that online services that meet the requirements for mere conduit, caching, or hosting must still comply with any court order to remove unlawful content.[99]

Liability Shield provisions for Intermediary

The United States has a separate law, the DMCA, that governs online copyright law. In the United States, the DMCA states that an online service is not liable for third-party content that violates copyright law if "upon obtaining such knowledge or awareness, it acts expeditiously to remove, or disable access to, the material." Once platforms become aware of potentially harmful or illegal content, it is often easier for platforms to remove it immediately to avoid liability rather than determine whether the content breaks any laws.

Japan is one of the most technologically advanced countries. It has also provided broad awareness protection to intermediaries, where intermediaries are not liable unless they have actual knowledge. Article 3 of Japan's Provider Liability Limitation Act, enacted in 2001, contains a liability shield that does not apply if a provider is aware that third-party content causes "the infringement of the rights of others," or if "there is a reasonable ground to find" that they know this.[100]

Instances of Businesses Exiting Markets Due to Increasing Regulations

In Hong Kong, with recent changes to data protection law[101] against the prevalent doxing where people put other person's personal information online so others can harass them[102], the law has prescribed criminal investigation and prosecution of the employees of tech companies for doxing offences by their users.[103] According to an industry coalition of tech companies based in Hong Kong, Facebook, Google and Twitter have reportedly already hinted at leaving the country if the proposed legislation prescribing criminal liability is implemented.[104]

According to these companies, refraining from investments and service offerings would only avoid sanctions on them under the proposed law.

In China, in October 2021, LinkedIn exited the Chinese market citing "challenging operating environment" as the cause when the Chinese government increased its scrutiny.[105] It is worth noting that

the Chinese Personal Information Protection Law was passed by the Chinese Standing Committee of the National People's Congress on August 20, 2021 and was effective from November 01, 2021.[106] The Article 71 of the law contains criminalising provisions that may have been a cause for LinkedIn's exit.

In India, META reportedly wanted to call it quits as it fears the data privacy law could force it to modify or cease existing business practices under the DP Bill, 2021 as it fears that it could face fines, orders restricting or blocking its services, or other government-imposed remedies as a result of content hosted on its platform.[107] Though the threat was later recalled, it still implies the sentiments of big digital businesses towards the regulatory landscape.

Large digital platforms, services, and marketplaces provide small businesses with affordable, scalable, and secure business solutions. They have opened up new markets and allowed small businesses to compete globally and in unimaginable ways a few decades ago.[108]

As per a recent report,[109] criminality was never a part of punitive action against businesses in ancient India, and only financial penalties were. If any of the intermediaries decide to leave India due to over-regulations and criminalisation; no matter how far-fetched the notion is, the first impact will be on thousands of small businesses that use these platforms. Small businesses are the backbone of the Indian economy and represent India's spirit of start-up India and innovation.

Way Forward

Criminalisation provisions are neither novel nor novice in the business regulations. A recently released report[110] highlighted 26,134 different ways of going to jail for doing business in India. This number is alarming because such provisions deter new businesses from entering the market in India and impact their operations and day-to-day functioning, thus making it difficult for the businesses to operate. As businesses aid the economy to grow, such criminalising provisions are harmful to the country's economy, which the government is trying to improve.

The criminal jurisprudence in the country finds it appropriate to place criminal liability on a business; by extension on its employees in higher-ranking positions. However, a company is a legal person and not a natural person cannot be ignored. A legal person devoid of intent; can only act on intent of its employees; and in cases of non-compoundable offences; should be liable to be punished.

Below are some recommendations that can be used to make the framework of criminality for digital businesses more conducive and less imposing.

Adoption of Civil Liability Framework

India will benefit from adopting a framework similar to Brazil's where instead of segregating social media companies through the number of users; a division of businesses or platforms can happen based on roles, responsibility and capacity.

Each case should be evaluated on a subjective basis on merit, and before such evaluation, no imprisonment of an employee or ascertaining of liability should be done. The instant FIR and imprisonment nudge the judicial system towards a 'guilty until proven innocent approach' as opposed to much accepted in India 'innocent until proven guilty approach'.

Liability Shield

Intermediaries must be shielded by law from liability for third Party Content as any rules governing intermediary liability must be provided by laws, which must be precise, clear, and accessible. Under the IT Act framework, intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in modifying that content. Similarly, a provision can be introduced under the Copyright Act to limit the liability of intermediaries not modifying the content to a notice-to-notice requirement. Suppose the IT Act and the Copyright Act incorporate similar notice-and-notice regimes. In that case, the amended Copyright Act may specifically provide that the responsibilities for intermediaries shall be governed by the provisions of Section 79 of the IT Act.

Laws with Imprisoning clauses must Satisfy the Test of Necessity and Proportionality

The sections with minor economic offences under the PSSA should be moved to a show-cause notice requirement. Sections 26(1) and (4) should be reassessed on the proportionality of punishment and then the sections should be decriminalised as per the Finance Ministry's proposal.

Section 85 under IT Act allows for directors to be held liable for any infringement of the Act along with Rule 7 of Intermediary Rules, 2021, with similar intent. The vague and ambiguous language of these sections must be amended and transparency and accountability be built into laws.

Rule 4 of Intermediary Rules 2021 specifies the specific qualification of the CCO, which borders on infringing in the internal business matters of a corporation. This section must be tested on the ground of proportionality and over-prescriptive regulations must be avoided. The test of Proportionality prescribed under the *Puttaswamy Judgement*[111] should be the cornerstone for any law that takes away any right.

Repealing laws without adequate safeguards to protect the interest of citizens and Intermediaries

Since a country's regulations are framed for the betterment of its citizens and economy, any law which does not provide adequate safeguard must be abolished in favour of a better law. As observed by the Supreme Court, Section 69 A of the IT Act alongside the Blocking rules has practically unused safeguards and should not remain in force for preventing misuse.

The Criminal sanctions on intermediaries for non-compliance with government orders under the Blocking Rules would need to be repealed as being disproportionate and creating a chilling effect on the freedom of expression.[112] The upcoming Data Protection Bill, 2021 places disproportionate responsibilities on digital businesses instead of the government, before being brought in force Section 85, similar to IT Act, would need to be assessed on vagueness, proportionality and necessity.

It is important that the regulator proceeds with the intent of promoting Ease of Doing Digital Business in India while framing new legislations and assessing the existing ones.

Endnotes

1 'India's trillion-dollar digital opportunity' *available at* India's Trillion Dollar Digital Opportunity

2 Baird, Forrest E. and Koffman, Walter. ìPhilosophic Classics Volume IV. Nineteenth-Century Philosophy.î 2nd Edition. Prentice Hall Press. Upper Saddle River, New Jersey. 2000.

3 Tiwari, Piyush, 'DOCTRINE OF PROPORTIONALITY: AN ANALYSIS OF SUPREME COURT CASES', October 13, 2018, Racolb Legal, *available at* Doctrine of Proportionality: An analysis of Supreme Court cases | RACOLB LEGAL

4 Tauro Lionel, 'India: The Limited Liability Of Intermediaries For Third Party Content', 7 April 2021, Mondaq, *available at* The Limited Liability Of Intermediaries For Third Party Content - Media, Telecoms, IT, Entertainment - India

5 Aiyar, Shankkar, 'Archaic laws criminalise entrepreneurs', 13 February 2022, The New Indian Express, *available at* Archaic laws criminalise entrepreneurs.

6 Press Trust of India, 'Govt steps improving India's ease of doing business rank: Commerce ministry', 24 October 2019, Business Standard, *available at* Govt steps improving India's ease of doing business rank: Commerce ministry | Business Standard News

7 Krishnan, KP and Ravi Venkatesan, 'Making business easy: A template to ramp-up state capacity', 17 June 2021, Economic Times, *available at* MSMEs: Making business easy: A template to ramp-up state capacity - The Economic Times

8 Tungekar, Bushra MS, 'Decriminalization of compoundable company law offences', 29 January 2021, *available at* Decriminalization of compoundable company law offences - iPleaders

[9] Govt clears amendments to LLP Act; to decriminalise 12 offences under law, 28 July 2021, Business Standard, *available at* Govt decriminalises Companies Act to promote greater ease of doing business | Business Standard News

[10] Murshedd, Suhana Islam, Mitra, Shounak, Ease Of Doing Business Gains Momentum With The Latest Amendments To The LLP Act, 21 February 2022, Mondaq, *available at* Ease Of Doing Business Gains Momentum With The Latest Amendments To The LLP Act - Corporate/Commercial Law - India

[11] Government of India Ministry of Finance Department of Financial Services *** 8th June, 2020 Statement of Reason: Decriminalisati

[12] Tandon, Suneera, 'Retailers urge DIPP to decriminalize LM Act', 16 December 2022, Mint, *available at* Retailers urge DIPP to decriminalize LM Act

[13] Section 79, IT ACt, 2000 *available at* Section 79 in The Information Technology Act, 2000

[14] Singh, Shubham, 'What does Section 79 of IT Act mean for social media intermediaries?', May 28, 2021, Zee News, *available at* Explained: What does Section 79 of IT Act mean for social media intermediaries? | Technology News | Zee News

[15] Pandey, Jyoti, 'The Supreme Court Judgement in Shreya Singhal and What It Does for Intermediary Liability in India?', 11 April 2015, Centre for Internet and Society, available at The Supreme Court Judgement in Shreya Singhal and What It Does for Intermediary Liability in India? — The Centre for Internet and Society

[16] Agarwal, Shubhra and Agarwal, Anusha, 'Section 67 of IT Act 2000: Scope, Misuse and the Striking Inadequacy', 2 June 2020, Criminal Law Blog National Law University, Jodhpur, *available at* Section 67 of IT Act 2000: Scope, Misuse and the Striking Inadequacy

[17] Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2004 (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427, *available at* Avnish Bajaj vs State on 29 May, 2008

[18] Ekta Kapoor v. State Of M.P, on 11.11.2020, Madhya Pradesh High Court, *available at* Ekta Kapoor vs State Of MP on 11 November, 2020

[19] 'Complaint against Ekta Kapoor's Alt Balaji dismissed due to lack of evidence by cyber police', 3 June 2020, PinkVilla, *available at* Complaint against Ekta Kapoor's Alt Balaji dismissed due to lack of evidence by cyber police | PINKVILLA

[20] 'Madhya Pradesh HC refuses to quash case against Ekta Kapoor', 12 November 2020, The Hindu, *available at* Madhya Pradesh HC refuses to quash case against Ekta Kapoor - The Hindu

[21] 'SC Grants Interim Protection From Arrest To Ekta Kapoor In FIR In 'XXX Season 2' Controversy', 17 December 2020, News ABP Live, *available at* SC Grants Interim Protection From Arrest To Ekta Kapoor In FIR In 'XXX Season 2' Controversy

[22] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, *available at* Procedure and Safeguards for Interception, Monitoring and Decryption

[23] Rule 21 under the 2009 Rules.

[24] Apar Gupta v. Ministry Of Home Affairs, Central Information Commission, *available at* Apar Gupta vs Ministry Of Home Affairs on 31 January, 2022

[25] 'Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State', 14 January 2019, The Wire, *available at* Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State

[26] Jalan, Pranay, 'Guest Post: Resolving the Good Samaritan Paradox: An Enabler for Proactive Content Moderation?', 1 October 2021, Indian Constitutional Law and Philosophy, *available at* intermediary liability – Indian Constitutional Law and Philosophy

[27] X v. Union of India and Ors., 20 April 2021, Delhi High Court *available* at X vs Union Of India And Ors. on 20 April, 2021

[28] ABC v. DEF and Ors., 24 September 2020, Delhi High Court, *available at* https://indiankanoon.org/doc/77617707/

[29] 'Information Technology (Intermediary guidelines and Digital media ethics Code) Rules, 2020' *available at* https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf

[30] Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016. available at Information Technology (Prese...r Facilities) Rules, 2016

[31] Regidi, Asheeta, 'The Indian Government proposes new data retention rules:will privacy be compromised?', 14 October 2016, First Post, *available at* The Indian government proposes new data retention rules: Will privacy be compromised?- Technology News, Firstpost

[32] Bharadwaj Deeksha, 'Centre may tweak IT Act, bring in new penalties', 16 September 2021, Hindustan Times, *available at* Centre may tweak IT Act, bring in new penalties | Latest News India - Hindustan Times

[33] Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73.

[34] 'Supreme Court Upholds Freedom of Speech on the Internet', Lexology, *available at* Supreme Court Upholds Freedom of Speech on the Internet - Lexology

[35] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, *available at,* Information Technology (Blocking Rules), 2009

[36] S, Aishwarya, 'Information Technology (Blocking Rules), 2009 and Section 69a of the IT Act, 2000', 22 November 2021, Ipleaders, *available at* Information Technology (Blocking Rules), 2009 and Section 69a of the IT Act, 2000 - iPleaders.

[37] Deol, Taran, 'All about Section 69A of IT Act under which Twitter had withheld several posts & accounts', 2 February, 2021, The Print, *available at* All about Section 69A of IT Act under which Twitter had withheld several posts & accounts

[38] Sabu Mathew George v. Union of India and Ors., *available at* Sabu Mathew George vs Union Of India And Ors. on 13 December, 2017

[39] Joshi, Divij, 'Indian Intermediary Liability Regime Compliance with the Manila Principles on Intermediary Liability', Centre for Internet and Society, *available at* Indian Intermediary Liability Regime

[40] 'India's Surveillance State', 2014, SLFC, *available at* https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf

[41] Regidi, Asheeta, 'The Indian Government proposes new data retention rules:will privacy be compromised?', 14 October 2016, First Post, *available at* The Indian government proposes new data retention rules: Will privacy be compromised?- Technology News, Firstpost

[42] Rule 2(w) under the Intermediary Rules, 2021.

[43] 'Govt sets 50 lakh users threshold to define 'significant social media intermediary' under IT rules', February 27, 2021, Economic Times, *available at* Govt sets 50 lakh users threshold to define 'significant social media intermediary' under IT rules - The Economic Times

[44] How the intermediaries' rules are anti-democratic and unconstitutional.

[45] To ensure compliance with the Information Technology Act, 2000 and Intermediary Rules.

[46] To ensure 24x7 coordination with law enforcement agencies to ensure compliance with orders made in accordance with law.

[47] To enforce redressal grievance mechanism as per Rule 3(2) of the Intermediary Rules.

[48] Under Rule 4(a) it is stated that The Chief Compliance officer can be made liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder. This is subject to an opportunity of being heard.

[49] 'Platforms with over 50 lakh users to be 'significant social media intermediaries', February 28, 2021, The Indian Express, *available at* Platforms with over 50 lakh users to be 'significant social media intermediaries' | Technology News,The Indian Express

[50] Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, *available at* Fat salary but bigger risks: Is this a tech job that nobody wants?

[51] Section 2(51) of Companies Act, 2013 gives the definition of Key Managerial Person.

[52] Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, *available at* Fat salary but bigger risks: Is this a tech job that nobody wants?

[53] 'Twitter transfers India head Manish Maheshwari to US, assigns new role of senior director', 13 August 2021, The Print, *available at* Twitter transfers India head Manish Maheshwari to US, assigns new role of senior director

[54] Incidents of lynching and mob violence have been reported from videos and messages circulated on the WhatsApp platform in India. For reference, *Viral WhatsApp Messages Are Triggering Mob Killings In India*, July 18, 2018, Lauren Frayer, *available at* Viral WhatsApp Messages Are Triggering Mob Killings In India : NPR

[55] Singh, Vikram Jeet; Mara, Prashant; India: Liable vs. Accountable: How Criminal Use Of Online Platforms And Social Media Poses Challenges To Intermediary Protection In India; May 2020; Mondaq; *available at* Liable vs. Accountable: How Criminal Use Of Online Platforms And Social Media Poses Challenges To Intermediary Protection In India - Media, Telecoms, IT, Entertainment - India

[56] October 2021 https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf

[57] Bharadwaj, Deeksha, 'Centre may tweak IT Act, bring in new penalties', September 16, 2021, Hindustan Times, *available at* Centre may tweak IT Act, bring in new penalties | Latest News India - Hindustan Times

[58] MouthShut.com v. Union of India, WRIT PETITION (CIVIL) NO. OF 2013, *available at* MouthShut.com v/s Union of India - Supreme Court - Freedom of Expression

[59] Authorisation for operations provided under Section 7, PSSA, 2007 *available at* Payment and Settlement Systems Act, 2007

[60] Section 4, PSSA, 2007 *available at* Payment and Settlement Systems Act, 2007

[61] 'Offences Which Do Not Provide a Minimum Sentence of 7 Years Imprisonment Are Not Heinous: SC', January 10, 2020, The Wire, *available at* Offences Which Do Not Provide a Minimum Sentence of 7 Years Imprisonment Are Not Heinous: SC

[62] Section 299, IPC, 1860.

[63] Whoever commits culpable homicide not amounting to murder, shall be punished with imprisonment for life, or imprisonment for either description of a term which may extend to 10 years.

[64] Obhan, Ashima and Dua, Akanksha, 'Decriminalization of Minor Economic Offences: A Step towards 'Sabka Saath, Sabka Vikas and Sabka Vishwas", 18 August 2020, Lexology, *available at* Decriminalization of Minor Economic Offences: A Step towards 'Sabka Saath, Sabka Vikas and Sabka Vishwas' - Lexology

[65] 'Cheque bouncing will no longer be criminal offence?', Babushahi Bureau, 12 June 2020, *available at* https://www.babushahi.com/full-news.php?id=103124&headline=Cheque-bouncing-will-no-longer-be-criminal-offence

[66] Recommendation 6, JPC Report on PDP Bill, 2019.

[67] Shreya Singhal v. Union of India, AIR 2015 SC 1523.

[68] Section 66A empowered police to make arrests over what policemen, in terms of their subjective discretion, could construe as "offensive" or "menacing" or for the purposes of causing annoyance, inconvenience, etc.

[69] Avinash Bajaj v. State, 2008 (150) DLT 769.

[70] My Space Inc. v. Super Cassettes Industries Ltd.,236 (2017) DLT 478.

[71] Tauro L (2021) The Limited Liability Of Intermediaries For Third Party Content. Mondaq, *available at* The Limited Liability Of Intermediaries For Third Party Content - Media, Telecoms, IT, Entertainment - India

[72] Section 69, Copyright Act, 1957, *available at* the copyright act, 1957 (14 of 1957)

[73] Google v. Visakha Industries, [Criminal Petition No. 7207 of 2009], *available at* Google India Private Ltd vs M/ S. Visakha Industries on 10 December, 2019

[74] Intermediary Liability 2.0: A Shifting Paradigm, SFLC, Licensed under CC BY-SA-NC 4.0, *available at* INTERMEDIARY LIABILITY 2.0: A SHIFTING PARADIGM

[75] Bharadwaj, Prachi, ' Google India fails to gain protection under Section 79 of the IT Act, 2000; To face trial in a 2008 defamation case', 11 December 2019, SCC Online, *available at* Google India fails to gain protection under Section 79 of the IT Act, 2000; To face trial in a 2008 defamation case | SCC Blog

[76] My Space Inc. vs Super Cassettes Industries Ltd, 23 December, 2016, Delhi high court, *available at* My Space Inc. vs Super Cassettes Industries Ltd. on 23 December, 2016.

[77] Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors, 18 January, 2017, Delhi High Court, *available at* Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors on 18 January, 2017.

[78] 'Liability of Online Intermediaries under the Copyright Regime', 10 February, 2021, Kashish IPR, *available at* Liability of Online Intermediaries under the Copyright Regime.

[79] Joshi, Neha, 'Alibaba.com moves Bombay High Court against account freezing in cheating case', 10 March 2022, Bar and Bench, *available at* Alibaba.com moves Bombay High Court against account freezing in cheating case

[80] Chen, Rong, 'Policy and Regulatory Issues with Digital Businesses', July 2019, World Bank Policy Research Working Paper 8948, *available at* Policy and Regulatory Issues with Digital Businesses

[81] Rule 4(1) (a) of Intermediary rules 2021.

[82] INTERMEDIARY LIABILITY, Center for Internet and Society, *available at* Intermediary Liability | Center for Internet and Society

[83] Canabarro, Diego Rafael and Real, Paula, Corte, 'Mapping Intermediary Liability in Latin America', 21 August 2020, Internet Society, *available at* Mapping Intermediary Liability in Latin America - Internet Society

[84] Zingales, Nicolo, 'The Brazilian approach to internet intermediary liability: blueprint for a global regime?', 28 December 2015, Internet Policy Review, DOI: 10.14763/2015.4.395, *available at* The Brazilian approach to internet intermediary liability: blueprint for a global regime? | Internet Policy Review

[85] Brazil's Superior Court of Justice, Fourth Panel, Google Brazil, Special Appeal no. 1306157/SP, 24 March 2014.

[86] 'Marco Civil da Internet - "Brazilian Civil Rights Framework for the Internet', 23 April 2014, WILMAP Stanford, *available at* Marco Civil da Internet - "Brazilian Civil Rights Framework for the Internet" | wilmap

[87] Bartz, Diane, 'Big tech supports global tax, but wants digital services levies axed', 9 June 2021, Reuters, *available at* Big tech supports global tax, but wants digital services levies axed | Reuters

[88] Zingales, Nicolo, 'The Brazilian approach to internet intermediary liability: blueprint for a global regime?', 28 December 2015, Internet Policy Review, DOI: 10.14763/2015.4.395, *available at* The Brazilian approach to internet intermediary liability: blueprint for a global regime? | Internet Policy Review

[89] Barata, John and Pappalardo, Kylie, 'Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021', 3 March 2021, Stanford, *available at* Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021 | wilmap

[90] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Japan, 2001), Article 3, Clause 2.

[91] 17 U.S. Code § 512 - Limitations on liability relating to material online, *available at* 17 US Code § 512 - Limitations on liability relating to material online

[92] *Ibid*.

[93] Electronic Communications and Transactions Act, 2002 (Republic of South Africa), Chapter XI, Section 77.

[94] Broadcasting Services Act 1992 (Commonwealth of Australia), Schedule 5, Clause 91.

[95] Google Inc v. ACCC (2013) 249 CLR 435, *available at* https://jade.io/j/?a=outline&id=289620

[96] In Hells Angels Motorcycle Corporation (Australia) Pty Ltd v. Redbubble Ltd (2019) 140 IPR 172, *available at* https://jade.io/j/?a=outline&id=638087

[97] Kamath, Raunak, 'Internet Committee Publishes Report on Intermediary Liability in Asia-Pacific Region', 10 November 2021, INTA, *available at* Internet Committee Publishes Report on Intermediary Liability in Asia-Pacific Region - International Trademark Association

[98] 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, *available at* 47 US Code § 230 - Protection for private blocking and screening of offensive material

[99] Electronic Communications and Transactions Act, Chapter XI, Section 73-75.

[100] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Japan, 2001), Article 3, Clause 1.

[101] Personal Data (Privacy) Ordinance, Hong Kong *available at* 0PºNÇŒ™e(Áy±–) h‹O0 Personal Data (Privacy) Ordinance

[102] Purnell, Newley, 'Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws', July 5, 2021, The Wall Street Journal, *available at* Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws - WSJ

[103] MacAllister, Julia M. , 'The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information' , 85 Fordham L. Rev. 2451 (2017). *Available at:* https://ir.lawnet.fordham.edu/flr/vol85/iss5/44

[104] Purnell, Newley, 'Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws', July 5, 2021, The Wall Street Journal, *available at* Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws - WSJ

[105] 'After LinkedIn's exit from China, will more companies follow suit?', October 16, 2021, Business Standard, *available at* After LinkedIn's exit from China, will more companies follow suit? | Business Standard News

[106] Personal Information Protection Law of the Mainland, *available at* Personal Information Protection Law of the Mainland

[107] 'Meta ready to throw in towel', 4 March 2022, India Business Law Journal, *available at* Meta ready to throw in towel | India Business Law Journal

[108] Ward, Jake, 'Digital big tech drives small business success', November 19, 2019, the Hill, *available at* https://thehill.com/opinion/technology/471005-digital-big-tech-drives-small-business-success

[109] 'Jailed for Doing Business', February 10, 2022, ORF, *available at* Jailed For Doing Business | ORF.

[110] 'Jailed for Doing Business', February 10, 2022, ORF, *available at* Jailed For Doing Business | ORF.

[111] Justice K.S.Puttaswamy(Retd) v. Union Of India, 26 September, 2018, *available at* Justice KSPuttaswamy(Retd) vs Union Of India on 26 September, 2018

[112] Joshi, Divij, 'Indian Intermediary Liability Regime Compliance with the Manila Principles on Intermediary Liability', Centre for Internet and Society, *available at* Indian Intermediary Liability Regime

5
CHAPTER

Impact of Regulatory Uncertainty on Ease of Doing Digital Business in India

Prince Gupta, Senior Research Associate, CUTS International

Overview

The government has taken several steps to foster a digital-first economy, including promoting the ease of doing business for digital businesses. However, the persisting regulatory uncertainty has adversely impacted the Ease of Doing Digital Business (EoDDB). The objective of the Discussion Paper is to emphasise the need of regulatory certainty by highlighting how regulatory uncertainty has impacted businesses in India in different sectors.

Regulating the digital economy becomes tougher due to its cross-cutting nature which causes regulatory overlaps. Further, the difficulty gets intensified due to lack of set regulatory procedures. The paper highlights the several reasons which cause regulatory uncertainty for digital businesses including lack of regulatory framework, excessive delay in enactment of regulations, arbitrary approach of regulators, sub-optimal or ambiguous design, incorrect interpretation and failure in effective and efficient implementation. The paper analyses of how regulatory uncertainty caused due to these factors affects the digital business from different sectors such as e-commerce, online gaming, ed-tech and fintech.

Regulatory uncertainty impacts both businesses and consumers and the government must take steps to curb it. For this, the paper argues for formulation of a principles-based regulatory framework, inspiration for which can be taken from the United Kingdom Government's Digital Charter. Further, the paper makes a case for adoption of a Whole of Government (WoG) approach and institutionalisation of set regulatory procedures. Furthermore, effective engagement with the Parliament to establish accountability of regulatory actions has been suggested. Creation of a mechanism for informal guidance is also recommended.

Introduction

In a market economy, regulation is considered a key government intervention for correcting imperfections and anomalies in the market. It involves laying down instructions about what business entities can or cannot do. In India, since the late 1990s, the government has set up independent regulatory agencies which have developed different approaches to regulate the economy and achieve their regulatory goals.[1]

Today, the Indian economy is rapidly changing as traditional business models are being transformed for digital adoption and new business models are being introduced. The digital economy has provided newer digital services to consumers which have only grown due to network effects.[2] While digital firms have provided numerous new innovative digital products and services to consumers, their growth has posed several challenges. For instance, consumers risk privacy invasion and are exposed to information disorder on social media platforms. Further, issues such as the rights of gig workers working for digital businesses and effective taxation of digital businesses which operate across borders are also present.

Thus, the government has been grappling with the challenge of regulating the new and rapidly expanding industries while safeguarding against potential risks. There is an increasing recognition of

digital businesses being seen as entities requiring specialised regulatory/policy interventions, and the government has taken steps for the same.

However, in several cases, the approach to regulation of the digital economy followed by the government has led to regulatory uncertainties. Regulatory uncertainty is defined as a condition of perceived inability of a business to predict the future state of the regulatory environment.[3]

Regulation is done by using different instruments, including making legislations and policies, framing subordinate legislation including regulations, guidelines, notifications, orders, and judicial decisions etc. These various actions are taken by the different arms of the state including the executive - central and state governments, the legislative – the parliament and state assemblies, the judiciary and quasi-judicial bodies, and the regulatory agencies.

When there is arbitrariness, ambiguity, inconsistency, instability and frequent changes in these different instruments used by the different arms of the state, it may lead to regulatory uncertainty. Such uncertainty may be because of multiple reasons including:

- lack of legal and regulatory framework and instruments,
- excessive delay in the enactment of proposed laws and regulations,
- arbitrary approach of issuing regulations,
- sub-optimal or ambiguous design of regulatory framework and instruments,
- incorrect interpretation of the regulatory instrument,
- failure in effective and efficient implementation of the regulatory instrument.

While the Ministry of Electronics and Information Technology (MeitY) has articulated a vision of the digital economy which states that regulatory policies should be supportive,[4] given its dynamic and ever-changing nature, regulatory uncertainty has only intensified with the government's arbitrary, ambiguous, inconsistent and unstable actions. It is essential to take a look at the reasons for this which are highlighted below:

Cross-cutting Nature of the Digital Economy and Regulatory Overlaps

Regulatory overlaps can occur when multiple regulatory agencies try to achieve similar goals, engage in similar activities and regulate similar entities.[5] Regulatory overlaps cause uncertainty, delays and poor enforcement.[6] This is because the different regulatory agencies may bring in conflicting sets of regulations and are often not able to resolve differences amicably in a time bound manner.[7] This causes delays which becomes a cause of regulatory uncertainty.

Various government ministries and regulators work to regulate the digital economy. Akin to traditional businesses, digital businesses are regulated under sectoral regulations, and are subject to the competition and consumer protection regimes. However, in addition to these, digital businesses are also subject to the India's cyber law, the Information Technology Act, 2000 (IT Act) and will also be subject to the proposed data protection law and other such legislations which may be enacted. Thus, the regulatory overlaps have become even more complicated in the digital economy because of its cross-cutting nature and involvement of data.

Apart from the government ministries and departments such as MeitY, Department of Consumer Affairs, Department for Promotion of Industry and Internal Trade (DPIIT), regulators such as the Telecom Regulatory Authority of India (TRAI), the Competition Commission of India (CCI), the Reserve Bank of India (RBI), and the Central Consumer Protection Authority (CCPA) regulate the digital economy.[8] There is another proposed horizontal regulator for data protection, the Data Protection Authority (DPA). Debates about having an e-commerce regulator[9] and a social-media regulator[10] are also on-going. Further, India also has agencies for cyber security such as Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC).

The lack of clarity among regulators about their jurisdiction, which stems from a lack of clarity about their objectives causes regulatory uncertainty and delays.[11] In the past, this has led to regulators reaching constitutional courts. A famous case is the CCI vs Bharti Airtel Limited where the Supreme Court laid out

the jurisdictions in which sectoral and horizontal regulators can operate.[12] However, conflicts may also arise between two horizontal regulators such as the CCI and the CCPA which may cause regulatory uncertainty. Conflicts between state agencies undermine the credibility and capacity of the state to regulate effectively. To prevent this, the Joint Parliamentary Committee's (JPC) Report on the Personal Data Protection Bill, 2019 (PDP Bill, 2019) mandates the DPA to consult with other regulators and authorities in case of concurrent jurisdiction which is a welcome step.

Lack of Set Regulatory Procedures across Regulators and their Arbitrary Approach

When different regulators do not have common set of regulatory procedures and standards for circulating consultation papers, inviting public comments, issuing regulations and evaluating the conduct of digital businesses, it results in them being flexible and adopting arbitrary approach of regulations where they may bring in ad-hoc regulations.[13]

Doctrine of Arbitrary State Action states that any arbitrary state action is against the principles of natural justice and is violative of Article 14 of the Constitution of India.[14] In the Cellular Operators Association v TRAI case, the Supreme Court held that TRAI's action of mandating one-rupee credits to subscribers for each call drop was manifestly arbitrary and violated the Article 14 and Article 19(1)(g).[15]

Impact of Regulatory Uncertainty on the Ease of Doing Digital Business

The government has recognised that 'a thriving digital economy needs a creative balance between regulation, compliance and innovation' and the 'ease of operation for digital businesses should drastically improve' which would require 'adopting supportive policies and regulations.'[16] The regulatory landscape is an important criterion for businesses to make investments.

In this context, a vast body of literature proves that the lack of regulatory certainty adversely impacts businesses' investment decisions. Uncertainty in proposed laws also hampers investment decisions.[17] Further, policy uncertainty can also affect the level of investment a firm makes. This is because the uncertainty associated with regulatory and policy changes adversely impacts a business's profitability.[18] Due to the irreversibility of investment decisions, businesses may also not invest as they would want to be wary of investing in activities that may lead to them losing their money.[19] Further, empirical research shows that policy and regulatory uncertainty temporarily reduces the output in the economy and employment levels and, thus, has an overall negative impact on the economy of any country.[20]

An example of this is the international e-commerce giant, Shopee's exit from the Indian market which, exited within six months of starting its operation citing 'global market uncertainties'. However, reports stated that the exit was influenced by the Indian government's banning of the Free Fire which is owned by Singapore-based Sea Group, the parent company of Shopee.[21] The arbitrary action of banning the app resulted in massive loss in market capitalisation for the Sea group.[22]

Thus, regulatory uncertainty is undesirable and an impediment to the development of the digital economy because it makes it difficult for digital businesses to make decisions. As digital markets are increasingly becoming powerful drivers of social and economic growth, the impact of digital regulation needs assessment.[23]

Regulation of the digital economy must be done to achieve greater public good. Today, governments across the world are adopting newer ways to regulate digital businesses and going forward, the regulatory pressure will only increase.[24]

In this context, it is also essential that a regulatory landscape that instils trust in businesses and in turn allows for better investment flows, business landscape, competitiveness and thus, increases the Ease of Doing Digital Business (EoDDB) is created.

Regulatory Uncertainty in Specific Sectors

To effectively create policy and regulatory certainty, it is important to understand and highlight how regulatory uncertainty persists in different sectors and impacts EoDDB. This section illustrates the existing regulatory uncertainties in a few specific sectors highlighting how digital businesses are impacted because of uncertainties.

1. Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021

Internet in India is currently governed under the IT Act and its rules which are brought from time to time to regulate the different aspects of the digital economy like cybersecurity, social media companies etc. The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) were released in February 2021 under the sub-section (3) of Section 69A, sub-section (2) of Section 79.[25]

The rules require social media intermediaries, as defined under the rules to follow certain mandates. Due to sub-optimal and ambiguous drafting, the rules have created more confusion rather than providing clarity for the industry. For instance, the rules state that "social media intermediary means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services." The definition is broad enough to cover business messaging platforms like Microsoft Teams and Slack, SaaS companies like Freshworks and Zoho etc which are not social media services.[26]

The IT Rules have also created ambiguity on what constitutes a messaging service. The rules state that any SSMI "proving services primarily in the nature of messaging" will have to identify the first originator of the information. As it was unclear how "primarily in the nature of messaging" will be defined for intermediaries as they may also provide different other services on their platform,[27] MeitY came up with a set of Frequently Asked Questions (FAQs) to bring clarity and explain nuances of due diligence in November, 2021.[28] Until then, digital companies struggled to ascertain if they would have to follow the provisions under the rules or not.

The FAQs stated that "online interaction" should be the primary or sole purpose while also detailing what qualifies as the primary purpose. While this has brought certainty for some digital business such as payment gateways and ed-tech platforms, uncertainty still exists.[29] It is unclear if rules are applicable on Apple iMessage or not because the service is exclusively offered to Apple users.[30]

Further, the rules require SSMIs primarily having messaging services to report the first originator of the information. While the government has claimed that for this purpose, the rules do not need digital businesses to break end-to-end encryption which messaging platforms provide, digital businesses have stated that it would be impossible for them to do so. It remains unclear how compliance will be ensured without breaking encryption, thus causing uncertainty. This has resulted in one of the messaging services, WhatsApp filing a petition in the Delhi High Court (HC) and stating that it will infringe "the fundamental right to privacy and free speech of citizens."[31]

Furthermore, the rules require digital media publishers to adhere to a Code of Ethics be subject to self-regulation with an oversight mechanism of the central government. Stating that regulatory provisions hamper free speech and appear to be aimed at "controlling the media by the government", the Madras HC and the Bombay HC have put a stay. It remains unclear whether the provisions applicable on the digital media publishers would apply on a print newspaper which also has an online edition as print newspapers are already regulated under Press Council of India norms.

2. Digital Taxation and Equalisation Levy

As digital businesses easily transcend borders, governments have introduced a digital services tax on foreign-based digital firms. India introduced Equalisation Levy (E.L.) 1.0 in 2016 putting a tax of six percent on digital advertisement services. This led to double taxation of digital businesses in India, complicating the taxation framework.[32]

E.L. 2.0 was introduced through in 2020 mandating foreign 'e-commerce operator' having 'online sale of goods' or 'online provision of service' to pay a two percent E.L on the gross revenue received from the provision of 'e-commerce supply or service' to Indian residents or non-resident companies with a permanent establishment in India. This introduction increased the complexity and uncertainty for businesses as what constitutes online sale of goods and online provision of service was left unclear which is an issue of sub-optimal drafting of regulations.

These were later clarified in the budget of 2021, when the scope of the E.L. was substantially increased. Until the Finance Bill 2021 was passed, the industry was in a state of uncertainty about the taxation. However, even now, the provisions of the are worded widely and vaguely such that they are open to interpretation to even cover the sale of physical goods as services.[33]

E.L. became a contentious issue for India after the US termed it discriminatory, unfairly targeting the American tech companies. It proposed a 25 percent retaliatory tariff on Indian products in May 2021.[34] However, negotiations began in June 2021 for a uniform international taxation system for digital businesses under the OECD and G20 and the US suspended the retaliatory tariff for six months.[35] In October 2021, 136 countries joined the framework. This is expected to add certainty and stability to the international tax system. However, until this tax deal comes into effect, India intends to continue imposing its 2-6 percent E.L.

In December 2021, India's Finance Minister, Nirmala Sitharaman stated that there should be a 'level of predictability' in tax rates for both direct and indirect taxes.[36] However, the uncertainty has led to major US digital companies deciding to not create deferred tax assets in their accounting statement until they get more clarity on the digital taxation.[37]

3. Regulation of Crypto-assets/ Virtual Digital Assets

The government has adopted an inconsistent approach in regulating cryptocurrencies which has created uncertainty for both, industry players and consumers. The inconsistent and arbitrary approach stems from a lack of a regulatory framework.

In 2013, the RBI had issued a circular warning the public against cryptocurrencies. In February 2017, the RBI again issued a circular and in late 2017, the Finance Ministry and the RBI clarified that the cryptocurrencies are not legal tender.[38] Two Public Interest Litigations were filed in the Supreme Court, one seeking a complete ban and another seeking regulation of cryptocurrencies.

Subsequently, in November 2017, the government constituted an expert committee to draft legislation on cryptocurrencies which did not suggest a ban.[39] At the same time, the RBI issued a circular restricting all banks from allowing transactions, which effectively led to a ban on cryptocurrencies in India.

Further, the expert committee released a new version, 'Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019', suggesting a complete ban. In March 2020, the Supreme Court overturned the RBI directive which prohibited trading in cryptocurrencies, indicating it to be disproportionate.[41]

In February 2021, Nirmala Sitharaman, the Minister of Finance reiterated in the Parliament that the government wished to ban cryptocurrencies. However, in March 2021, she publicly stated that the government wants to foster innovation in the crypto space. Later in the year, the Standing Committee on Finance met crypto industry representatives and suggested that cryptocurrencies should be regulated and not banned. Subsequently, 'The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021' (Crypto Bill 2021) was listed to be tabled in the parliament in the winter session 2021. However, it was not introduced.[42]

The RBI arbitrarily banned cryptocurrencies in April, 2018 without any public consultation. The move led to cryptocurrency prices falling, frozen crypto exchanges and withdrawals being completely stopped.[40] The measures affected businesses and consumers who had invested in cryptocurrencies as their money froze and they became concerned about the steps the government would take for regulating the industry.

The Finance Ministry in the Union Budget 2022 termed cryptocurrencies as virtual digital assets and put a 30 percent tax on income from them and a one percent additional tax deduction at source (TDS). Despite taxation put in place, the ministry has issued a clarification that this move does not make crypto assets legal or illegal in India.[43] Further, throughout this time, the stance of the RBI has been to ban cryptocurrencies in India as they may be a threat to the macroeconomic stability of the country, while it is itself working on its own fiat digital currency.[44]

Due to the regulatory uncertainty in the sector, reportedly, companies have to restructure their strategies. In November, 2021, with the listing of the Crypto Bill, 2021, many crypto exchanges suspended ads for a couple of weeks and restarted when the government clarified that the bill would seek to not ban but regulate crypto-assets.[47] The crypto exchanges took a conservative approach and stopped advertising because they wanted to minimise their risks.[48]

Such regulatory uncertainty has escalated the difficulty in leveraging the potential of such digital technologies. When regulatory uncertainty increases, businesses often relocate to more favourable jurisdictions, and may take human talent with them.[45] For instance, a crypto based start-up, Polygon's co-founder highlighted that the digital businesses are affected by regulatory uncertainty in India. It is unfeasible for them to expose their teams to local risks, including their business being shut down. This results in brain drain where Indian talent chooses to move out of India.[46]

As per a recent report, the Finance Ministry is working on a consultation paper to deal with the issue of crypto assets and it will release the paper for public consultation in six months.[49] The industry body, Blockchain and Crypto Assets Council also wants to have more consultations with the government.[50]. Further, this is in concurrence with the G20 countries' effort to form a global consensus on the issues of regulatory arbitrage in the evolving digital developments including crypto-assets.[51] Reports suggest that the government will only frame the law after having a global consensus.[52] This has reduced the regulatory uncertainty for the sector.

4. Regulation of the E-Commerce Sector

As per the Allocation of Business Rules released in 2018, the e-commerce industry is to be regulated by the DPIIT, Ministry of Commerce and Industry. The Department of Consumer Affairs had released rules for protection of consumers in the e-commerce space. Moreover, the legal recognition of e-commerce is under the Ministry of Electronics and Information Technology (MeitY).[53] All these bodies define e-commerce differently[54] which creates regulatory uncertainty.

The Consumer Protection (E-commerce) Rules 2020[55] (E-commerce Rules 2020) and the proposed draft Consumer Protection (E-commerce) (Amendment) Rules 2021 (E-Commerce Amendment Rules 2021) were brought to prevent unfair trade practices in e-commerce and protect the interests and rights of consumers.[56] However, the proposed amendment rules were riddled with sub-optimal drafting. For instance, they introduced 'flash sale' which is contemplated as something which offers 'high discounts', 'significantly reduced prices' or other such promotions for a specific time period. However, there is ambiguity and uncertainty surrounding the phrase 'flash sale' as terms such as 'significantly reduced prices', 'high discounts', interception of 'ordinary course of business', have not been defined by the proposed amendment leaving the definition open to several subjective interpretations.[57] Even after the clarification in the press release in June, 2021, that third-party sellers' flash sales are not banned, the ambiguity in the definition is creating confusion.[58]

Further, regulatory uncertainty increases if different government bodies, having overlapping jurisdictions, work without much collaboration. For instance, reports highlight that there was a significant difference in opinion within the government for regulation and consumer protection in the e-commerce space which resulted in inconsistent and frequent changes in regulations which causes regulatory uncertainty.[59] Some of the provisions in the proposed E-commerce Amendment Rules 2021 like abuse of dominance overlap with provisions of Competition Law 2002, which has created ambiguity and thus regulatory uncertainty.[60] Various government departments including the Ministry of Finance, DPIIT, Ministry of Corporate Affairs, MeitY, and NITI Aayog had expressed their concerns about the potential of the

proposed rules to hurt ease of doing business, creating policy uncertainty, regulatory overlaps, similar compliances for e-commerce entities under different rules/laws, etc., which are largely targeted at e-commerce entities.[61]

Further, the Foreign Direct Investment (FDI) policy in e-commerce categorises e-commerce into marketplace-based e-commerce entities and inventory-based e-commerce entities. The proposed E-Commerce Rules Amendment 2021 restrict related parties of a marketplace-based e-commerce entity to be enlisted as sellers. However, the rules have not been notified yet. The uncertainty caused due to this has impacted business and investment decisions in the e-commerce space.[62] For instance, Tata delayed the launch of its super app since September 2021 because it was unclear if the app was classified as marketplace-based e-commerce or inventory-based e-commerce. In case of being classified as an e-marketplace, associated brands of Tata would not be able to sell products on the platform.[63] Further, plans for super app by the Adani Enterprises has also been impacted.[64]

Further, the DPIIT has been working on the National E-Commerce Policy and released a draft version in 2019. In early 2020, media reports referred to a newer version of the National E-Commerce Policy which suggested creation of a new e-commerce regulator.[65] Since then, there have been no developments in this regard. Reports have highlighted that the government wishes to release the National E-Commerce Policy and the new e-commerce rules for consumer protection together, in order to reduce the scope of misunderstanding and thus limit ambiguity.[66] While this approach can reduce regulatory uncertainty as conflicting set of regulations will not be issued, a significant delay in releasing the same would mean that businesses will hold on to their investments negatively impacting consumer choice.

5. Regulation of Online Gaming Sector

There are different types of online games such as fantasy sports, poker, rummy, etc. Online games may be categorised as 'games of skill' which are games where a player plays against other players and applies a strategy and 'games of chance' which games where a player plays against 'the house' and a strategy won't help the player. Here, betting and gambling are characterised as games of chance.[67]

Different petitions have been filed in different HCs seeking ban online gaming and fantasy sports. Responding to these petitions, the Punjab and Haryana HC in 2017, the Bombay HC in 2019 and the Rajasthan HC in 2021 have held that fantasy sports is a game of skill.[68] The Rajasthan HC also held that online gaming is a legitimate business activity under Article 19(1)(g) of the Constitution.[69] In August, 2021, the Supreme Court, stating that the fantasy sports have an element of skill that predominantly affects their outcome, upheld Rajasthan HC's judgement.[70]

While the above-mentioned judgements were in response to petitions filed for banning online gaming, laws were not made in these states. As betting and gambling are under state list of the 7th schedule of the Constitution of India, state governments can enact laws to ban games of chance. The regulatory landscape for the online gaming industry in India has been uncertain because there is an inconsistent interpretation of the terms 'game of skill' and 'game of chance' which has led to differential regulations by different state governments.[71] Many states have effectively banned online gaming stating such games to be games of chance.

Telangana was the first state to ban online gaming in 2017, followed by Andhra Pradesh in 2020. Governments of Tamil Nadu, Kerala and Karnataka have also taken steps to ban online gaming. This has created uncertainty for businesses to invest and expand, as they fear that many states may follow suit, and existing business investments may be threatened.[72]

However, the gaming industry through various petitions has been seeking clarity on the distinction between the game of chance and game of skill. Different petitions have been filed, challenging the laws brought to ban games of chance and gambling. The petitions, filed in different HCs, principally have stated that treating a game of skill under the game of chance category is arbitrary. For instance, Kerala government sought to ban online rummy through an amendment in the Kerala Gaming Act, 1960. The Kerala HC however held struck down the law stating that the law was unconstitutional and in violation of the fundamental rights to trade and commerce under Article 19(1)(g) and the right to equality under Article 14 of the Constitution of India.[73]

The Karnataka State Assembly had passed the Karnataka Police (Amendment) Act, 2021 prescribing a ban on online gaming which was struck down by the Karnataka HC. The Karnataka Government has moved to the Supreme Court against this.[74] Similarly, the Tamil Nadu State Assembly had passed the Tamil Nadu Gaming and Police Laws (Amendment) Act of 2021 which was struck down by the Madras HC. The HC stated the government can make a new law to regulate the industry. Now, the Tamil Nadu Government has stated that it will go to the Supreme Court against the Madras HC's order.[75] On the other hand, governments of Rajasthan, Maharashtra and Telangana have stated that they wish to regulate the industry[76] which is a positive stance.

Experts have opined that since online gaming is free flowing and transcends state boundaries, a central driven national framework will bring in regulatory certainty and clarity which will inspire businesses to grow and innovate.[77] There have been some developments at the union level. While online gaming has been considered outside the ambit of the central government, in July 2018, the 276th Law Commission had suggested that the central government may bring in a legislation for regulating online games under the entry 31 of List 1 of 7th Schedule of the Constitution of India since online games are offered over digital platforms.

Following this, the Sports (Online Gaming and Prevention of Fraud) Bill, 2018 ("Sports Bill") was introduced as a private member bill in Lok Sabha in December, 2018 by the Lok Sabha MP Shashi Tharoor. The bill aimed to prevent and penalise frauds and also regulate online sports betting activities.[78] NITI Aayog also came up with 'Guiding Principles for the Uniform National-Level Regulation of Online Fantasy Sports Platforms in India' in December 2020.[79]

Lately, a uniform approach towards regulation is under consideration by the central government.[80] In the winter session of 2021 of the Parliament, the Lok Sabha Member of Parliament, Sushil Kumar Modi raised his voice stating the need of regulating the online gaming industry.[81] However, these developments have not led to a national policy or legislation which can create parity across the country for the regulation of the gaming industry.

The inconsistent interpretation of the terms 'game of skill' and 'game of chance' create ambiguity and uncertainty about the future and status of online gaming. Experts have opined that this leads to a decrease in the investment as there is a sense of uncertainty.[82] The industry has seeking clarity on several provisions of such legislation.[83] Further, currently, the industry largely remains self-regulated and has formed several associations such as the All-India Gaming Federation, The Online Rummy Federation, and the Federation of Indian Fantasy Sports.[84] However, there also have been calls for setting up a single self-regulatory body which can provide certainty to foreign investors and thus help drive innovation, employment and taxes.[85]

6. Regulation in the Ed-Tech Sector

There has been an increasing call for regulation of the ed-tech sector in India. The Lok Sabha Member of Parliament, Karti Chidambaram raised the issue of ed-tech platforms engaging in predatory marketing practices in the winter session in 2021 in the Parliament.[86] Subsequently, the Ministry of Education released an advisory to citizens in December, 2021 detailing out the dos and don'ts for students and their guardians and also stated that ed-tech companies are e-commerce entities and need to comply with the Consumer Protection (E-Commerce) Rules, 2020.[87]

The Education Minister announced that a policy to regulate ed-tech companies was in works in January, 2022.[88] Following this, before stricter norms being put in place by the government, ed-tech companies formed the India EdTech Consortium and prepared a code of conduct for self-regulation which was shared with the officials from the Ministry of Education.[89] The ministry has decided to closely track the code of conduct enforcement by the ed-tech companies.[90] Even after the industry opting for self-regulation and the ministry recognising it, there is no clarity if the ministry is still working on a policy for regulation. This further causes regulatory uncertainty for the ed-tech industry.

7. Regulation for Fintech Industry

Given the growth of fin-tech sector, the RBI has set up a dedicated fintech department in order to identify challenges and opportunities in the sector and facilitate innovation.[91] However, given the regulatory approach of the RBI in the past, digital businesses have faced uncertainty about compliance to regulatory norms.[92] For instance, recently, the RBI had mandated processing of e-mandate on cards for recurring transactions and card on file tokenisation through different circulars. These circulars were issued without conducting inclusive stakeholder consultation and thus resulted in uncertainty about the role different kinds of business entities would have to play for compliance. This resulted in lack of industry's readiness to adhere to the directives, ultimately resulted in consumers facing inconvenience.[93]Such unintended adverse consequences could have been avoided by following an inclusive stakeholder consultation.

Further, in the digital lending sector, digital businesses have been uncertain of the regulatory stance of the regulator and focused on existing customers as opposed to increase their customer acquisition.[94] While RBI's Report of the Working Group on 'Digital Lending including Lending through Online Platforms and Mobile Apps' has been released,[95] regulations are yet to be issued. Now, the National Payment Council of India (NPCI) has sought RBI's permission to enable credit through Unified Payment Interface (UPI). However, there exists a need for regulatory clarity for Merchant Discount Rate (MDR) for credit-based UPI transactions.[96]

The RBI had also mandated interoperability for all full-Know Your Customer prepaid payment instruments (PPI) including prepaid payment wallets.[97] However, fintech firms remained uncertain about the level of compliance required and the MDR they could charge, and hence missed the deadline. [98]

Regulatory uncertainty also exists with respect to data localisation and cross border data flows norms mandated by the RBI. However, the expanse of the topic demands a separate paper and thus, will be covered in detail in an upcoming paper on cross border data flows in this discussion paper series.

Recommendations and the Way Forward

Regulation of an industry is typically a combination of executive, legislative and judicial actions of the three branches of the government. Thus, bringing in regulatory certainty is a difficult task. However, good regulation is a step towards building a safer internet world. The developmental pace of digital technologies challenges regulation making.[99] The need for optimum regulations persists and steps should be taken to work on the reasons which lead to regulatory uncertainty. This section illustrates a few recommendations for this purpose.

The United Kingdom (UK) formulated a Digital Charter[102] in 2018 by bringing together the government, the industry and the civil society. The Charter has specified three different work programmes on (i) making online space safe, (ii) making work technology for society as a whole and (iii) to promote fair and efficient digital markets. It further details out what the UK government had done for each of these work programmes and what it needs to do more while also setting out guiding principles and goals to be achieved.

1. Formulate a principles-based Regulatory Framework

As the digital economy is dynamic, there is a requirement of change in regulations from time to time.[100] Thus, the government should first design guiding principles and adopt a principle-based regulatory framework. The design of legislations and regulations should be done based on the guiding principles with an aim to achieve the intended policy goals.

The government has articulated its vision for the growth of the digital economy which recognises the need for supportive policies and regulations. Further, the Minister for MeitY, Ashwini Vaishnaw and the Minister of State for MeitY, Rajeev Chandrashekhar have also articulated their vision for the regulation of the digital economy in various public platforms.[101] However, the government has not worked with different stakeholders to create an official regulatory framework. This formulation, when done with due public consultation, can result in development of a better umbrella framework and other countries such as the UK has followed this.

In India, the RBI framed a Payment Systems Vision 2019-21 with public consultation which was a step in positive direction.[103] However, the digital economy covers aspects much more than just the payment sectors and therefore needs an overarching framework. Hence, the government should do due public consultation and create an official principles-based regulatory framework.

2. Adopt a Whole of Government (WoG) Approach

Even after having a principles-based regulatory framework, regulatory enforcement is a challenge.[104] Regulation is adversely impacted when there is regulatory overlap and there is a need to minimise these overlaps.[105] To effectively tackle this, dialogue between the different government departments and agencies is important and must. Hence, a WoG approach must be adopted so that these departments and agencies work jointly to resolve issues of regulation.

Further, as big digital businesses transcend sectoral boundaries, regulators need capacity building. Therefore, adopting a WoG approach will also enable the government to bring in its expertise from different departments before making regulations and enforcing them. Further, different regulators have been set up at different instances for achieving different kinds of results, collaborating on different issues becomes difficult. Therefore, new regulatory collaboration methods should be designed so that in cases of regulatory overlaps, regulation is not compromised due to turf wars.

To facilitate this process, guidelines for adopting a WoG approach and regulatory collaboration must be made by the government. A Policy Convergence Unit may be formed and can be housed in NITI Aayog.[106] However, while adopting this approach, the independence of regulators must be respected and not interfered with.

3. Institutionalise Set Regulatory Procedures

The lack of set regulatory procedures and standards leads to regulators following arbitrary approach of regulation. This causes regulatory uncertainty. There is a need to institutionalise regulatory procedures followed by different regulators. This should include mandating the regulators to conduct due public consultation, justifying the reasons the issued regulation in writing and following regulatory impact assessment, among others.

Adopting transparency in regulation making can cut arbitrary regulations.[107] For this purpose, regulators should indulge in public consultation with stakeholders like industry associations, businesses and consumers and be responsive to comments received by the public. This practice can lead to lower levels of regulatory uncertainty.[108] The degree to which this is followed also indicates how well the rule of law is observed.[109] Studies show that when regulatory agencies take time to change the regulatory landscape, regulatory uncertainty is reduced and there are more opportunities for investments and innovation.[110]

In the Cellular Operators Association v TRAI case,[111] the Supreme Court referenced the Airports Economic Regulatory Authority of India Act, 2008 which requires the authority under the act to perform public consultation and maintain transparency. The court found a lack of transparency in the consultation process carried out by TRAI. Without making 'upholding transparency' in the regulatory process a general requirement, the court expressed its desire for the Parliament to step in and enact legislation similar to the Administrative Procedure Act, 1946 (AP Act) of the US.[112]

In this context, the absence of legislation that sets out procedures and standards for regulation on the lines of the AP Act in the United States is an impediment to effective regulation.[113] Under the AP Act, regulators are required to mandatorily give a general notice of any rulemaking in the federal register, conduct public consultation and provide standards for judicial review.[114] The AP Act is successfully checks arbitrary actions in regulation making and thus helps create regulatory certainty.[115] In India, though there exists a Pre-Legislative Consultation Policy, it is not followed in spirit.[116] Further, efforts to bring a law for this purpose like the Regulatory Reform Bill in 2013[117] and the Pre-Legislative Consultation Bill in 2021[118] have not been able to materialise.

Regulatory Impact Assessment (RIA) is an approach to ensure that suboptimal results are not achieved.[119] Different reform commissions including Financial Sector Legislative Reforms Commission, Damodaran Committee Report and the Tax Administration Reform Commission, among others have

suggested adopting RIA.[120] However, the same has not been made mandatory for all regulators in India. In many jurisdictions, regulatory agencies are required to conduct RIA mandatorily.[121]

Light touch regulation can facilitate innovation, thus adopting light but tight regulations should be encouraged.[122] Sunset clauses may also be put in these regulations so that contextually irrelevant regulations end naturally without any requirement of repealing them. Further, to clear regulatory uncertainty and confusion, different regulators can also conduct public meetings periodically, say once in 3 months, to make their stance on regulatory aspects public, like the Monetary Policy Committee of the RBI.

Further, regulations may be first tested using regulatory sandboxes.[123]

Furthermore, regulators may also encourage the usage of technology for reducing regulatory uncertainty. This can include digital businesses using regulatory technology (regtech) to comply with regulations and regulators utilising supervisory technology (suptech) to meet regulatory objectives and ensure compliance by digital businesses.[124] When technological tools are used effectively for achieving these ends, it can result in an overall better regulatory system which minimises regulatory uncertainty. These tools range from digital platforms, machine learning, blockchain etc. In India, steps in this direction are already being taken by other regulators such as the Food Safety and Standards Authority of India (FSSAI) which has digitalised its licensing and registration functions, re-designed its portal as Food Safety Compliance System (FoSCoS) for intelligent decision making.[125]

4. Mechanism for Informal Guidance

Given the constant innovations in the space of digital economy, digital businesses have wish to seek clarity on regulatory aspects before taking a business decision. In this regard, regulators should allow digital businesses to approach them for seeking clarifications. This is already present in the fields like taxation where businesses can reach the Board for Advance Ruling[126] and securities market where Security and Exchange Board of India (SEBI) has the Informal Guidance Scheme.[127] Here, businesses receive the guidance about the consequences of a proposed decision. Adoption of this practice by regulators will aid in reducing regulatory uncertainty. While such guidance should not become precedence, it can still provide regulatory certainty to businesses about the thinking of the regulator.[128]

5. Effectively Engage the Parliament for Establishing Accountability

Regulators should be made accountable for not maintaining regulatory certainty. For this purpose, the parliament should be actively engaged for establishing their accountability. Even though laws have the provisions for parliamentary committees reviewing the work on regulatory agencies, in practice, this is found missing. The departmentally related standing committees only carry out macro level scrutiny.[129] An enhanced parliamentary review of actions of regulators by standing committees can help establish accountability and thus bring in regulatory certainty. In this regard, legal reforms should be carried out, mandating a dedicated standing committee to review delegated legislation. The Parliamentary Committee on Subordinate Legislation may be designated for this purpose.[130]

6. International Cooperation between Governments

There are several challenges for which governments across the world take steps to cooperate and learn from each other and further work jointly to effectively fight them. A good example of this is the finance and banking sector. Over the years, central banks of different countries have come together to form the Bank of International Settlements which has helped form regulations in the form of Basel norms for tackling world economic crises.[131]

As digital businesses often transcend territorial boundaries, they also pose regulatory challenges to governments across the world. Governments should come together to form *guiding principles* so that the digital economy is effectively regulated. The OECD led International Regulatory Co-operation helps governments with adding an international lens to rulemaking.[132] A similar body should be made focused towards the digital economy. Cooperation may also be done at regional or bilateral levels and other countries have taken a step in this direction. For instance, the Association of Southeast Asian Nations

(ASEAN) is working on a Digital Economy Framework Agreement, negotiations for which are said to be completed by 2025.[133] The US and EU have also worked on the transatlantic Data Privacy Flows.[134]

This step will drastically help the digital economy as regulatory uncertainty will reduce because of governments adopting similar guiding principles for regulation. However, this should not result a one-size-fits all approach as different countries are in different stages of the evolution of the digital economy. Rather than harmonisation of approaches, cooperation must lead to coherence.

Endnotes

1 Vakil Raeesa, 'Indian Administrative Law and the Challenges of the Regulatory State' in 'Regulation in India Design, Capacity, Performance by Devesh Kapur and Madhav Khosla', April 04, 2019, Bloomsbury Publishing.

2 'Could Regulation put the Brakes on the Digital Economy?', Bearing Point, *available at:* https://www.bearingpoint.com/en/our-success/insights/could-regulation-put-the-brakes-on-the-digital-economy/

3 Hoffmann Volker H., Trautmann Thomas and Hamprecht Jens, 'Regulatory Uncertainty: A Reason to Postpone Investments? Not Necessarily', September 2009, Journal of Management Studies, *available at:* https://doi.org/10.1111/j.1467-6486.2009.00866.x

4 'India's Trillion-Dollar Digital Opportunity', February 2019, Ministry of Electronics and Information Technology, *available at:* https://www.digitalindia.gov.in/ebook/MeitY_TrillionDollarDigitalEconomy.pdf

5 Reducing Regulatory Overlap in the 21st Century, May 2019, Business Roundtable, *available at:* https://s3.amazonaws.com/brt.org/BRT.Reducing-RegulatoryOverlapinthe21stCentury.2019.05.31.pdf

6 *Ibid;* 'Regulating the Regulators', December 2013, The Hindu Business Line, *available at:* https://www.thehindubusinessline.com/opinion/regulating-the-regulators/article64592319.ece

7 Kelkar Vijay L and Mehta Pradeep S, 'Why we need to save administration from administrators', The Economic Times Online, *available at:* https://economictimes.indiatimes.com/opinion/et-commentary/view-why-we-need-to-save-administration-from-administrators/articleshow/87937440.cms

8 Sharan Vivan and Kalawatia Mohit, 'Rationalize Regulatory Overlaps to Unleash our Digital Economy', September 16, 2020, Mint, *available at:* https://www.livemint.com/opinion/online-views/rationalize-regulatory-overlaps-to-unleash-our-digital-economy-11600270679178.html

9 Nandi Shreya, 'Govt may set up independent regulatory authority for e-commerce sector', August 14, 2021, Business Standard, *available at:* https://www.business-standard.com/article/markets/govt-may-set-up-independent-regulatory-authority-for-e-commerce-sector-121081302135_1.html

10 Pradhan Bibhudatta, 'Parliamentary panel recommends new regulator for social media platforms like Facebook, Twitter', November 24, 2021, The Economic Times, *available at:* https://m.economictimes.com/news/economy/policy/parliamentary-panel-recommends-new-regulator-for-social-media-platforms-like-facebook-twitter/articleshow/87885446.cms

11 Roy Shubho, Shah Ajay, Srikrishna B.N. and Sundaresan Somasekhar, 'Building State capacity for regulation in India', August 03, 2017, Working Paper Series, National Institute of Public Finance and Policy, *available at:* https://www.nipfp.org.in/media/medialibrary/2018/08/WP_237_2018_0cilwuT.pdf

12 Gupta Swasti, 'Analysis of Competition Cases in India: Competition Commission of India V. Bharti Airtel Limited and Ors.', October-December 2018, CUTS, *available at:* https://cuts-ccier.org/pdf/Edition-11-Analysis_of_Competition_Cases_in_India.pdf

13 *Supra at 1.*

14 Maneka Gandhi v. Union of India, AIR 1978 SC 597, *available at:* https://indiankanoon.org/doc/1766147/

15 Cellular Operators Association v Telecom Regulatory Authority of India (2016) 7 SCC 703, *available at:* https://indiankanoon.org/doc/116404795/

[16] https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

[17] Wagner Helmut, 'Costs of Legal Uncertainty: Is Harmonization of Law a Good Solution?', January 2009, Discussion Paper No. 444, University of Hagen, *available at:* https://www.fernuni-hagen.de/wirtschaftswissenschaft/download/beitraege/db444.pdf; Williams Richard, 'The Impact of Regulation on Investment and the U.S. Economy', Mercatus Center at George Mason University, *available at:* https://www.mercatus.org/system/files/House%20Oversight%20Response%20on%20Regulations%20and%20Economy%5B2%5D.pdf

[18] Kingsley Allison F., Vanden Bergh Richard G., and Bonardi Jean-Philippe, 'Political Markets and Regulatory Uncertainty: Insights and Implications for Integrated Strategy', July 25, 2012, Symposium, Academy of Management Perspectives, *available at:* https://journals.aom.org/doi/abs/10.5465/amp.2012.0042

[19] Dixit Avinash and Pindyck Robert S., 'Investment under Uncertainty', 1994, Princeton University Press, *available at:* https://press.princeton.edu/books/hardcover/9780691034102/investment-under-uncertainty

[20] Sinclair Tara M. and Xie Zhoudan, 'Sentiment and Uncertainty about Regulation', June 2021, GW Regulatory Studies Center, George Washington University, *available at:* https://regulatorystudies.columbian.gwu.edu/sentiment-and-uncertainty-about-regulation-0; Baker Scott R., Bloom Nicholas and Davis Steven J., 'Measuring Economic Policy Uncertainty', July 2016, Quarterly Journal of Economics, *available at*: https://academic.oup.com/qje/article/131/4/1593/2468873; Anand Rahul and Volodymyr Tulin, 'Disentangling India's Investment Slowdown', March 24, 2014, International Monetary Fund Working Papers, *available at:* https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Disentangling-Indias-Investment-Slowdown-41436

[21] Barik Soumyarendra and Mukul Pranav, 'Explained: Why has Shopee shut shop in India?', March 29, 2022 The Indian Express: *available at:* https://indianexpress.com/article/explained/shopee-exit-india-operations-explained-7842028/

[22] Poh Olivia, and Lee Yoolim, 'Sea's Market Decline Hits $132 Billion as Stock Tumbles Again', March 2022, Bloomberg, *available at:* https://www.bloomberg.com/news/articles/2022-03-02/sea-s-market-decline-hits-132-billion-as-stock-tumbles-again

[23] Sundberg Nancy, 'Digital regulation:7 ways to move the cursor', February 15, 2021, International Telecom Union, *available at:* https://www.itu.int/en/myitu/News/2021/02/15/10/44/Digital-regulation-7-ways-to-move-the-cursor

[24] Foroohar Rana, 'Big Tech braces for a year of regulatory pressure', January 19, 2022, Financial Times, *available at*: https://www.ft.com/content/825eca35-8bf1-47dd-814a-8e22f40e6761

[25] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology, *available at:* https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[26] Mathi Sarvesh, 'How The IT Rules FAQs Add To The Arbitrariness And Confusion Around The Rules', November 3, 2021, Medianama, *available at:* https://www.medianama.com/2021/11/223-it-rules-faqs-arbitrariness/

[27] *Ibid.*

[28] Frequently Asked Questions (FAQs) The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 202, Ministry of Electronics and Information Technology, *available at:* https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf

[29] Mathi Sarvesh, 'How the IT Rules FAQs Add to The Arbitrariness and Confusion Around the Rules', November 3, 2021, Medianama, *available at:* https://www.medianama.com/2021/11/223-it-rules-faqs-arbitrariness/

[30] Jain Anushka, 'Are the IT Rules Applicable to Apple's IMessage? Here's What an RTI Has Revealed', July 16, 2021, Medianama, *available at:* https://www.medianama.com/2021/07/223-it-rules-apple-imessage-rti-compliance/

[31] 'WhatsApp vs Indian govt on IT rules: Can encryption be broken, who is right, who is wrong', May 27, 2021, India Today, *available at:* https://www.indiatoday.in/technology/features/story/whatsapp-vs-indian-govt-on-it-rules-can-encryption-be-broken-who-is-right-who-is-wrong-1807649-2021-05-27

[32] Gupta Vidushi, 'Decoding the maze of equalisation levy', March 30, 2021, The Hindu Business Line, *available at:* https://www.thehindubusinessline.com/opinion/decoding-the-maze-of-equalisation-levy/article34200358.ece; 'Wider ramifications of Equalisation Levy 2.0', Oct 03, 2021, The Hindu Business Line, *available at:* https://www.thehindubusinessline.com/business-laws/wider-ramifications-of-equalisation-levy-20/article36813363.ece

[33] *Ibid*

[34] Sen Amiti, 'USTR to terminate proposed retaliatory action against India's digital tax', November 25, 2021, The Hindu Business Line, *available at:* https://www.thehindubusinessline.com/news/national/ustr-to-terminate-proposed-retaliatory-action-against-indias-digital-tax/article37677197.ece

[35] *Ibid*

[36] 'Next Union budget may retain focus on infrastructure story: Nirmala Sitharaman', December 05, 2021, Hindustan Times, *available at:* https://www.hindustantimes.com/india-news/next-union-budget-may-retain-focus-on-infrastructure-story-finance-minister-nirmala-sitharaman-101638643942050.html

[37] Dave Sachin, 'Big Tech firms play it safe, await clarity before adjusting India taxes', February 10, 2022, The Economic Times, *available at:* https://economictimes.indiatimes.com/tech/technology/big-tech-firms-play-it-safe-await-clarity-before-adjusting-india-taxes/articleshow/89463122.cms

[38] Qureshi Mehbab, 'A look at cryptocurrency's journey so far in India', November 30, 2021, The Indian Express, *available at:* https://indianexpress.com/article/technology/crypto/cryptocurrency-in-india-a-look-at-the-regulatory-journey-of-cryptocurrencies-7648767/;

'Cryptocurrencies In India: A Battle with Government Diktats, RBI Warnings', June 10, 2018, NDTV, *available at:* https://www.ndtv.com/business/cryptocurrencies-bitcoins-battle-with-government-diktats-rbi-warnings-1865290

[39] Draft Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019, PRS Legislative Research, *available at* https://prsindia.org/billtrack/draft-banning-of-cryptocurrency-regulation-of-official-digital-currency-bill-2019

[40] *Supra at 38.*

[41] Krishnan Murali, 'Supreme Court rejects RBI ban on cryptocurrency biz', March 05, 2020, Hindustan Times, *available at:* https://www.hindustantimes.com/business-news/supreme-court-rejects-rbi-ban-on-cryptocurrency-biz/story-xjdpIRJtScBv64kcu4ToBI.html

[42] Mankotia Anandita Singh, 'Cryptocurrency Bill may not be introduced this Winter Session', December 16, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/economy/policy/cryptocurrency-bill-may-not-be-introduced-in-winter-session/articleshow/88288077.cms

[43] Chadha, Sunaina, '30% tax on income from digital assets: All you need to know', February 01, 2022, The Times of India, *available at:* https://timesofindia.indiatimes.com/business/india-business/30-tax-on-digital-assets-all-you-need-to-know/articleshow/89267925.cms

[44] 'RBI Board discusses private cryptocurrencies, CBDC', December 17, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/economy/policy/rbi-board-discusses-private-cryptocurrencies-cbdc/articleshow/88341119.cms

[45] Kalra Jaspreet, 'The Indian crypto brain drain: more headline than reality', March 16, 2022, The Ken, *available at:* https://the-ken.com/tokenised-edition/the-indian-crypto-brain-drain-more-headline-than-reality/

[46] *Ibid.*

[47] Mittal Apoorva, 'WazirX, Bitbns hit pause on crypto ads', November 17, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/tech/technology/wazirx-bitbns-hit-pause-on-crypto-ads/articleshow/87747630.cms

[48] Ghosh Monica, 'Regulatory uncertainty has not slowed down India's crypto sector', January 27, 2022, Forkast, *available at:* https://forkast.news/regulatory-uncertainty-not-slowed-india-crypto-sector/

[49] Mishra Asit Ranjan, 'Finance ministry working on consultation paper to deal with crypto assets', March 14, 2022, Business Standard, *available at:* https://www.business-standard.com/article/markets/finance-ministry-working-on-consultation-paper-to-deal-with-cryptoassets-122031300845_1.html

[50] Mahanta Vinod, 'Need more consultations with government to sort out operational issues: Crypto exchanges', February 09, 2022, The Economic Times, *available at:* https://economictimes.indiatimes.com/tech/technology/need-more-consultations-with-government-to-sort-out-operational-issues-crypto-exchanges/articleshow/89442757.cms

[51] *Supra at 49*.

[52] Beniwal Vrishti, 'India Will Frame Cryptocurrency Law Only After Global Consensus', April 2022, BloombergQuint, *available at:* https://www.bloombergquint.com/crypto/india-will-frame-cryptocurrency-law-only-after-global-consensus

[53] *Supra at 8*.

[54] E-Commerce, Legal Perspective', https://www.icsi.edu/media/webmodules/E-Commerce_LegalPerspective.pdf

[55] Consumer Protection (E-Commerce) Rules, 2020, Department of Consumer Affairs, *available at:* https://consumeraffairs.nic.in/sites/default/files/E%20commerce%20rules.pdf

[56] Sharma Mukul, Khandelwal Ishita, Garg Sanchit and Tambi Astha, 'Safe Harbour Protection for E-Commerce platforms', July 15, 2021, Cyril Amarchand Mangaldas, *available at:* https://corporate.cyrilamarchandblogs.com/tag/consumer-protection-e-commerce-rules-2020/

[57] Kumar Ujjwal, 'CUTS Comments on The Draft Amendments of the Consumer Protection (E-Commerce) Rules, 2020', CUTS, *available at:* https://cuts-ccier.org/pdf/cuts-comments-on-the-draft-amendments-of-the-consumer-protection-rules-2020.pdf

[58] *Ibid*.

[59] 'Significant difference of opinion within government on draft e-commerce rules: Official', September 22, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/economy/policy/significant-difference-of-opinion-within-government-on-draft-e-commerce-rules-official/articleshow/86425361.cms

[60] Singh Didar and Sinha Vidushi in 'Emerging Concerns about the E-Commerce Ecosystem in India in the Evolving Digital Economy' in 'India Competition and Regulation Report 2021' by Mehta Pradeep S, Kumar Ujjwal and Sodhi Garima, 2022, CUTS, *available at:* https://cuts-ccier.org/pdf/Report-ICRR2021.pdf

[61] 'Significant difference of opinion within government on draft e-commerce rules: Official', September 22, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/economy/policy/significant-difference-of-opinion-within-government-on-draft-e-commerce-rules-official/articleshow/86425361.cms; Mukul Pranav, 'Draft e-commerce rules: Industry dept objects, Niti Aayog chief says will hit ease of business', October 1, 2021, The Indian Express, *available at:* https://indianexpress.com/article/business/draft-ecommerce-rules-industry-dept-objects-niti-aayog-chief-says-will-hit-ease-of-business-7544824/

[62] 'Regulatory effectiveness in the era of digitalisation', June 2019, OECD, *available at* https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf

[63] Mathi Sarvesh, 'Why Tata Is Delaying The Launch Of Its Super App And Why This Matters?', September 2, 2021, Medianama, *available at:* https://www.medianama.com/2021/09/223-tata-super-app-delay-ecommerce-rules/

[64] 'Draft rules threaten to roil super-app plans for Tatas and Adanis', August 21, 2021, The Economic Times, *available at:* https://m.economictimes.com/industry/services/retail/draft-rules-possibly-ruins-super-app-plans-for-tatas-and-adanis/articleshow/85508642.cms

[65] Singh Didar and Sinha Vidushi in 'Emerging Concerns about the E-Commerce Ecosystemin India in the Evolving Digital Economy' in 'India Competition and Regulation Report 2021' by Mehta Pradeep S, Kumar Ujjwal and Sodhi Garima, 2022, CUTS, *available at:* https://cuts-ccier.org/pdf/Report-ICRR2021.pdf

[66] Anand Shambhavi, 'Draft ecommerce policy, rules to be released together soon', December 30, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/industry/services/retail/draft-ecommerce-policy-rules-to-be-released-together-soon/articleshow/88578236.cms

[67] Alawadhi Neha, 'Skill vs chance argument weighs as Indian states mull banning online gaming', October 19, 2021, Business Standard, *available at:* https://www.business-standard.com/article/technology/skill-vs-chance-argument-weighs-as-indian-states-mull-banning-online-gaming-121101901445_1.html

[68] Jolly Sachit, MP Priyanka and Roy Pritthish, 'Legal matrix of Online Fantasy Sports in India', November 24, 2020, Bar and Bench, *available at:* https://www.barandbench.com/columns/legal-matrix-of-online-fantasy-sports-in-india-2

[69] Avinash Mehrotra v. The State of Rajasthan & Ors., SLP (C) No. 18478/2020 *available at:* https://indiankanoon.org/doc/139194482/

[70] 'Supreme Court upholds Dream11 fantasy sports format as game of skill', August 04, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/tech/startups/supreme-court-upholds-dream11-fantasy-sports-format-as-game-of-skill/articleshow/85040855.cms

[71] Sahoo Sudhansu and Bajpai Suyash, 'Differential State Regulations On Online Fantasy Sports Platforms', December 30, 2020, Mondaq, *available at:* https://www.mondaq.com/india/gaming/1020724/differential-state-regulations-on-online-fantasy-sports-platforms

[72] Singh Shelley and Sharma Disha, 'Skill or chance? The USD7 billion question that can make or break India's online gaming industry.', October 27, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/prime/technology-and-startups/skill-or-chance-the-usd7-billion-question-that-can-make-or-break-indias-online-gaming-industry-/primearticleshow/87263751.cms

[73] Sharma Nalini, 'Online rummy a game of mere skill: Kerala High Court lifts state govt's ban', September 27, 2021, India Today, *available at:* https://www.indiatoday.in/law/story/online-rummy-game-of-skill-kerala-high-court-lifts-state-govt-ban-1857965-2021-09-27

[74] Roy Debayan, 'Karnataka moves Supreme Court challenging High Court verdict striking down law against online gaming', March 28, 2022, *available at:* https://www.barandbench.com/news/litigation/karnataka-moves-supreme-court-challenging-high-court-verdict-striking-down-law-against-online-gaming

[75] Bhan Indu, 'Tamil Nadu govt moves SC against HC order banning online betting games', December 8, 2021, The Financial Express, *available at:* https://www.financialexpress.com/industry/tn-moves-sc-against-hc-order-banning-online-betting-games/2384040/

[76] 'Rajasthan looks to explore fantasy sports sector; FIFS calls it a move in positive direction', March 09, 2022, Times Now News, *available at:* https://www.timesnownews.com/sports/esports/article/rajasthan-looks-to-explore-fantasy-sports-sector-fifs-calls-it-a-move-in-positive-direction/862109; 'Online Gaming Fraud: Maharashtra Government To Regularize Online Gaming', March 24, 2022, Times Now News, *available at:* https://www.timesnownews.com/videos/mirror-now/society/online-gaming-fraud-maharashtra-government-to-regularize-online-gaming-latest-updates-video-90421790; Tewari Saumya, 'Telangana to implement new norms for self-regulation of fantasy gaming', August 25, 2021, Mint, *available at:* https://www.livemint.com/sports/news/telangana-to-implement-new-norms-for-self-regulation-of-fantasy-gaming-11629905232908.html

[77] 'Experts recommend single self-regulatory body for online skill gaming', March 12, 2021, The Times of India, *available at:* https://timesofindia.indiatimes.com/business/india-business/experts-recommend-single-self-regulatory-body-for-online-skill-gaming/articleshow/81463088.cms

[78] Laghate Gaurav, 'Shashi Tharoor moves bill to regulate online gaming', January 15, 2019, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/economy/policy/shashi-tharoor-moves-bill-to-regulate-online-gaming/articleshow/67534323.cms

[79] 'Guiding Principles for the Uniform National-level Regulation of Online Fantasy Sports Platforms in India', December 2020, NITI Aayog, *available at:* https://www.niti.gov.in/sites/default/files/2020-12/FantasySports_DraftForComments.pdf

[80] https://www.medianama.com/2021/08/223-rti-government-online-gambling-regulation/

[81] Modi Sushil Kumar, 'Why online gaming in India needs regulation', December 29, 2021, The Indian Express, *available at:* https://indianexpress.com/article/opinion/columns/why-online-gaming-in-india-needs-regulation-7695383/

[82] 'Experts recommend single self-regulatory body for online skill gaming', March 12, 2021, The Times of India, *available at:* https://timesofindia.indiatimes.com/business/india-business/experts-recommend-single-self-regulatory-body-for-online-skill-gaming/articleshow/81463088.cms

[83] Rekhi Dia, 'Industry bodies seek clarity on online gaming', October 15, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/india/industry-bodies-seek-clarity-on-online-gaming/articleshow/87048341.cms

[84] Majumdar Debleena, 'Regulating ed-tech firms: will the much-needed guard rails choke innovation?', January 25, 2022, The Economic Times, *available at:* https://economictimes.indiatimes.com/prime/technology-and-startups/regulating-ed-tech-firms-will-the-much-needed-guard-rails-choke-innovation/primearticleshow/89098630.cms

[85] Sharma Yogita Seth, 'Online gaming industry seeks self-regulatory body for governing sector', January 18, 2021, The Economic Times, *available at:* https://economictimes.indiatimes.com/industry/media/entertainment/online-gaming-industry-seeks-self-regulatory-body-for-governing-sector/articleshow/80327777.cms

[86] 'Karti Chidambaram questions practices of edtech platforms like Byju's', December 14, 2021, The News Minute, *available at:* https://www.thenewsminute.com/article/karti-chidambaram-questions-practices-edtech-platforms-byju-s-158718

[87] 'Advisory to citizens regarding use of caution against Ed-tech Companies', December 23, 2021, Press Bureau of India, *available at:* https://pib.gov.in/PressReleasePage.aspx?PRID=1784582

[88] Barman Sourav Roy, 'Govt to track conduct code enforcement by edtech firms', January 19, 2022, The Indian Express, *available at:* https://indianexpress.com/article/india/govt-to-track-conduct-code-enforcement-by-edtech-firms-7730799/

[89] Choudhury Deepsekhar, and Abrar Peerzada, 'Edtech needs to self-regulate before strict norms enter the scene: Industry', December 25, 2021, Business Standard, *available at:* https://www.business-standard.com/article/companies/edtech-needs-to-self-regulate-before-strict-norms-enter-the-scene-industry-121122500021_1.html

[90] *Supra at 83.*

[91] 'RBI sets up fintech dept', January 10, 2022, The Times of India, *available at:* https://timesofindia.indiatimes.com/business/india-business/rbi-sets-up-fintech-dept/articleshow/88797179.cms

[92] Gupta Kapil, Sinha Vidushi and Gupta Prince, 'Consumer Welfare in Digital Payments', September, 2021, CUTS, *available at:* https://cuts-ccier.org/pdf/policy-brief-digital-payments.pdf

[93] *Ibid*; 'Implementation of RBI's Tokenisation Directive in Consumer Interest (CoFT Project)', December 2021, CUTS, *available at:* https://cuts-ccier.org/implementation-of-rbis-tokenisation-directive-in-consumer-interest-coft-project/

[94] Bhalla Tarush, 'Digital lenders focus on existing customers as uncertainty continues', July 14, 2020, Mint, *available at:* https://www.livemint.com/industry/banking/digital-lenders-focus-on-existing-customers-as-uncertainty-continues-11594726130683.html

[95] 'Report of the Working Group on digital lending including lending through online platforms and mobile apps', November 18, 2021, Reserve Bank of India, *available at:* https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52589

[96] 'Credit through UPI: Need for regulatory clarity', March 22, 2022, Ikigai Law, *available at:* https://www.ikigailaw.com/credit-through-upi-need-for-regulatory-clarity/

[97] Ghosh Debangana, 'Fintechs remain uncertain on implementing PPI interoperability, miss deadline', March 31, 2022, The Hindu Business Line, *available at:* https://www.thehindubusinessline.com/money-and-banking/fintechs-remain-uncertain-on-implementing-ppi-interoperability-miss-deadline/article65278732.ece

[98] *Ibid*.

[99] Malyshev Nick and Kauffmann Céline, 'Regulatory effectiveness in the era of digitalisation', June 2019, OECD Regulatory Policy Division, *a*vailable at: https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf

[100] *Ibid*.

[101] Aryan Aashish, Mathew Liz, 'Rajeev Chandrasekhar: 'Need to relook laws to de-risk Indian internet, make it difficult for Big Tech to be weaponised", March 28, 2022, The Indian Express, *available at:* https://indianexpress.com/article/business/interview-with-minister-of-state-for-electronics-and-it-7839701/; 'Need legal structure that balances freedom of expression, cyber regulation: Ashwini Vaishnav', April 5, 2022, The Indian Express, *available at:* https://indianexpress.com/article/india/need-legal-structure-that-balances-freedom-of-expression-cyber-regulation-ashwini-vaishnav-7852975/

[102] 'UK Policy Paper Digital Charter', 2018, Department for Digital, Culture, Media & Sport, United Kingdom, *available at:* https://www.gov.uk/government/publications/digital-charter/digital-charter

[103] 'Payment and Settlement Systems in India: Vision 2019 – 2021', May 15, 2019, Reserve Bank of India, *available at:* https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=47045

[104] 'Regulatory effectiveness in the era of digitalisation', June 2019, OECD, *available at:* https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf

[105] Kathuria Rajat, Kedia Mansi, Varma Gangesh and Bagchi Kaushambi, 'Economic Implications of Cross-Border Data Flow', November 2019, Indian Council for Research on International Economic Relations, *available at:* https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf

[106] 'India Competition and Regulation Report 2021' by Mehta Pradeep S, Kumar Ujjwal and Sodhi Garima, 2022, CUTS, *available at:* https://cuts-ccier.org/pdf/Report-ICRR2021.pdf

[107] Malyshev Nick, 'The Evolution of Regulatory Policies in OECD Countries', OECD, *available at:* https://www.oecd.org/gov/regulatory-policy/41882845.pdf

[108] Burman Anirudh and Zaveri Bhargavi, 'How Responsive Are India's Regulators?', April 19, 2021, BloombergQuint, *available at:* https://www.bloombergquint.com/law-and-policy/how-responsive-are-indias-regulators

[109] *Ibid*.

[110] Benthany A. Davis Noll, 'Judicial Review of Regulatory Policy in The Trump Era', 2021, Administrative Law Review, *available at:* https://www.law.nyu.edu/sites/default/files/DavisNoll-TiredofWinning_0.pdf

[111] Cellular Operators Association v Telecom Regulatory Authority of India (2016) 7 SCC 703, *available at:* https://indiankanoon.org/doc/116404795/

[112] Reddy K Vivek, 'Constitutional Regulation of the Fourth Branch' in 'Regulation in India Design, Capacity, Performance by Devesh Kapur and Madhav Khosla', April 04, 2019, Bloomsbury Publishing.

[113] *Supra at 1*.

[114] Administrative Procedure Act, 1946, United States of America, *available at:* https://www.justice.gov/sites/default/files/jmd/legacy/2014/05/01/act-pl79-404.pdf

[115] Benthany A. Davis Noll, 'Judicial Review of Regulatory Policy in The Trump Era', 2021, Administrative Law Review, *available at:* https://www.law.nyu.edu/sites/default/files/DavisNoll-TiredofWinning_0.pdf

[116] PS Arun, 'The need for a proper Pre- Legislative Consultation Policy', November 26, 2021, The Hindu, *available at:* https://www.thehindu.com/news/national/the-need-for-a-proper-pre-legislative-consultation-policy/article37677558.ece

[117] Sharma Seth Yogita, 'Government approves draft Regulatory Reform Bill', December 13, 2013, The Economic Times, *available at:* https://economictimes.indiatimes.com/news/economy/policy/government-approves-draft-regulatory-reform-bill/articleshow/27252539.cms

[118] Vasudev Antara and Manish Mayank, 'How Mandatory Public Consultations Can Help Draft Nuanced, More Transparent Laws', December 20, 2021, The Quint, *available at:* https://www.thequint.com/voices/opinion/no-legislation-without-consultation-a-look-at-the-pre-legislative-consultation-bill#read-more

[119] 'Regulatory Impact Assessment – A CUTS Note', 2015, CUTS, *available at:* https://cuts-ccier.org/pdf/Draft_Brief_Note_CUTS_on_RIA.pdf

[120] *Ibid*.

[121] *Supra at 1*.

[122] *Supra at 8*.

[123] Shashidhar KJ, 'Regulatory Sandboxes: Decoding India's attempt to Regulate Fintech Disruption', May 20, 2020, ORF Issue Brief, *available at:* https://www.orfonline.org/research/regulatory-sandboxes-decoding-indias-attempt-to-regulate-fintech-disruption-66427/

[124] Chandra Dakshina, 'Designing Technology Centric Regulators: Identifying Challenges to Regulatory Technology in India', September 30, 2021, Regulatory Governance Project National Law School of India University, *available at:* https://www.reg-gov.nls.ac.in/s/Designing-Technology-Centric-Regulators-in-India.pdf

[125] 'Food Safety and Compliance System (FoSCoS): Guidance Document', March 2, 2020, FSSAI, *available at:* https://foscos.fssai.gov.in/assets/docs/FoSCoSGuidanceDocumentV1_0_Latest.pdf

[126] 'Government sets up board for advance rulings in income tax matters', September 06, 2021, Mint, *available at:* https://www.livemint.com/news/india/government-sets-up-board-for-advance-rulings-in-income-tax-matters-11630927060473.html; 'Advance rulings can now be sought by e-mail', January 19, 2022, Mint, *available at:* https://www.livemint.com/news/india/advance-rulings-can-now-be-sought-by-email-11642607926502.html

[127] Loona RS, 'SEBI's Informal Guidance Scheme needs revamp', March 15, 2012, The Economic Times, *available at:* https://economictimes.indiatimes.com/sebis-informal-guidance-scheme-needs-revamp/articleshow/12270626.cms

[128] Singh Vijay Kumar, 'Informal Guidance Scheme of SEBI: Understanding the Concept and Analyzing the Guidance Provided by SEBI', March 2009, Taxmann's SEBI and Corporate Laws, *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1351132

[129] *Supra at 1*.

[130] *Supra at 1*.

[131] 'About Bank of International Settlements', *available at:* https://www.bis.org/about/index.htm?m=1_1; 'History of the Basel Committee', available at: https://www.bis.org/bcbs/history.htm

[132] 'International Regulatory Co-operation - Transforming rulemaking to meet the global challenges of the 21st century', OECD, *available at:* https://www.oecd.org/gov/regulatory-policy/irc.htm

[133] 'ASEAN Economic Community Council endorses roadmap to accelerate economic recovery, digital economy integration', October 21, 2021, ASEAN, *available at:* https://asean.org/asean-economic-community-council-endorses-roadmap-to-accelerate-economic-recovery-digital-economy-integration/

[134] 'Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo', March 25, 2022, European Commission, *available at:* https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443

6
CHAPTER

Impact of Unnecessary Compliances Ease of Doing Digital Business in India

Neelanjana Sharma, Senior Research Associate, CUTS International

Overview

In the Ease of Doing Digital Business (EoDDB) in India Study, we have undertaken a discussion paper series focusing on factors that impact digital businesses and their ease of doing business (EoDB) in India. India is at the cusp of a digital transformation and is seeking to see exponential growth in the digital economy, specifically US$800bn, by the year 2030.[1] This paper sets up a regulatory guillotine framework which is used for reviewing regulations for assessing unnecessary compliances.

Further, the paper with the help of box stories and examples from the contemporary regulatory landscape, renews the discussion on unnecessary compliances, costs associated, and their impact on digital businesses. It concludes with recommendations for simplifying, amending and repealing unnecessary compliances and installing good regulatory practices such as *'One in One out'* of the Great Britain to reduce compliance cost and institutionalising Regulatory Impact Assessment in the law-making process.

Introduction

Digital Businesses are leading technology-led innovations in recent times, and they require a regulatory environment that is easy to navigate. Laws of the country must not be a means of adding unnecessary compliances. This enables markets to have more innovation and competition while facilitating EoDDB in India. In a traditional setting, multiple compliance requirements come with large volumes of paperwork and a hostile environment for small businesses, which are the main causes behind the unease of doing business.[2]

To reduce the compliance burden, the centre has adopted a strategy of *elimination, simplification and decriminalisation*, which will have a multiplier effect on the ease of doing business.[3]

Along with the pandemic, the adoption of digital technology has been tremendous. The world we knew and experienced changed entirely. The pandemic became a business accelerator and all the services and businesses somewhere digitised and those already digital grew exponentially.[4] There has been a shift in consumer sentiment in a positive direction towards online channels and the industry and businesses have responded in turn.[5]

In a recent report by Red Seer, it was stated that India's consumer-based digital economy will become a US$800bn market by the year 2030.[6] This aligns with the country's vision to create a trillion-dollar economic value from the digital economy in 2025, half of which will be from new digital ecosystems.[7]

The Ministry of Electronics and Information Technology (MeitY) report stated the importance of capturing this value of the economy through decisive, significant, and speedy action by the Government of India (GoI). The GoI will need to work with the business sector to implement the enabling factors of policies and platforms in partnership with the business sector.[8]

The MeitY report states that the government is committed to drastically improving the ease of operations and reducing operating costs for digital businesses. This is being done to make India one of the 50 easiest countries for doing business.[9]

In the 2018 MeitY report, it was asserted that India should be one of the easiest countries to start a business for global digital businesses and start-ups. It also stated that compliance requirements should become purely digital and may require minimal time.[10] One of the issues left untouched then and until now was the nature and number of compliances and the increased cost of compliances for digital businesses.

India is one of the most cyber-branded countries owing to its human potential, capabilities, and contributions. With increasing risks and threats, India needs to have greater and stronger digital governance, code of ethics, regulations, and laws.[11]

Through this paper, we want to illustrate the meaning of unnecessary compliances in the context of today's digital world and businesses. Also, to outline the potential impact of such compliances on businesses in the form of their operations and cost to businesses. In doing so, it cannot be said that these alone are the compliance requirements for digital businesses, as most compliances for traditional businesses already apply to digital businesses. In order to further understand the impact, we will take up regulations aimed at digital businesses, both proposed and existing and highlight compliances that are a hindrance and can be reduced for promoting EoDDB in India. Towards the end of this paper, we will lay out some recommendations for reducing unnecessary compliances.

Unnecessary Compliances and what they mean for digital businesses

Reduction of compliance burden is the best way to strengthen & boost the confidence of business owners

– Piyush Goyal

The GoI has taken a mission to enhance the Ease of Doing Business (EoDB) in India. Under these reforms, one activity is to reduce business compliance as numerous regulatory compliances only confuse new prospects and build hesitations in investors.[12]

This warrants an understanding of regulatory compliances and when they become burdensome. Regulatory compliance can be defined as an organisation's adherence to laws, regulations, guidelines, and specifications for its business processes. Usually, violations can result in legal punishments.[13]

The compliances under laws and regulations cover each industry and with the constantly evolving regulatory environment, the target of compliance is constantly moving for businesses. This means that compliance requirements keep increasing, changing and multiplying. These changes in compliance requirements constantly occur and add to business uncertainty.[15] This need for constant adaptability of businesses becomes challenging, as compliances help businesses protect their reputation and resources.

However, businesses often complain about the regulations and costs of these compliances.[16] The usual solution that comes from such complaints is deregulation; however, the evolution of society and the internet and social risks of de-regulation cannot be ignored. To protect consumers and the market from the risks of digital evolution, the best way taken is to protect both economic growth and public welfare.[17]

In the 12 months up to December 31, 2021, there have been 3,577 regulatory changes for businesses. This translates to an average of 10 regulatory changes every single day.[14]

Not all compliances are unnecessary, but all compliances impose a burden on a business's resources. To ease this burden, only necessary compliances should exist.

The Challenge of Compliance

The influence of compliances is on all businesses; however, it can be an increasingly complex issue for small businesses. Small businesses, along with big digital businesses, are not exempt from data privacy regulations, cross-border flows, and payment regulations. However, these businesses are subject to disproportionate costs for compliances compared to larger corporations.[18]

As per a 2020 report[19] the biggest challenges an organisation's compliance teams face are regulatory change, budget and resource allocations and data protection. With increasing changes in regulations, compliances increase and so does the cost of compliance. Slowly, governments across the globe and GoI have understood the impact of increased compliances and their cost on businesses.

Though compliances can be burdensome, not all are unnecessary. As mentioned above, the Central Government had launched an initiative to reduce the compliance burden through the three-step process of simplification, elimination and decriminalisation. This study has already released a paper on decriminalising digital business provisions out of the three steps. In this paper, we cover unnecessary compliances or lack any legitimate reason and are burdensome on resources of any digital business.

The Centre government 2021 took various measures to reduce compliance burdens and facilitate EoDB and Ease of Living (EoL) in India.[20] It remains to be seen if the same can be said for digital businesses. The past regulatory interventions by the government have increased the compliance of some digital businesses. For instance, the new law on data protection which has been in the works for quite some time now, will bring in new compliances for digital businesses. These might include identifying data into categories and the appointment of new officers as the new law might shape up.[21] Once introduced the law would require start-ups to rethink their data handling practices, factor-in significant compliance costs.[22]

Components of Regulatory Compliance

There are various compliance burdens that digital businesses face in the country's regulatory landscape. Regulations are enforced via reporting or documentation processes that businesses need to undertake. The more complex the compliance requirements are, the more time, effort, and financial cost businesses incur. The financial cost associated with compliance can be straightforward to quantify, but regulators may not adequately appreciate that time is money.[23]

The study has a set scope. For this paper, the compliance burdens for digital businesses can be assessed on the cost of compliance. Each compliance, be it filing, recruiting, auditing or another, will have a cost component. This cost component, as defined below, can be broken into components of salaries of people recruited, compliance time, the cost for logistics and planning, and cost of administrative nature, including cost and time filing paperwork.[24]

Compliance costs refer to all of the expenses a company must incur in making sure they adhere to industry regulations. The compliance costs include the payroll for the compliance department, regulatory reporting costs, and any systems required for the process. Compliance costs for a company increase as the company expands globally and the regulation standards in an industry increase. [25]

It is noteworthy that digital businesses also have compliances with traditional businesses and their digital roles.

The more complex the regulations and compliance requirements, the greater is the disadvantage of small business entities which do not have dedicated regulatory affairs teams or financial muscle to deal with them.[26] In India, an average business is expected to meet 25,537 central compliances, and if a company operates in all states, it has to follow 69,233 compliances.[27]

Potential Unnecessary Compliance Burdens

Recently, Goa has recognised the need to ensure EoDB for start-ups and Information Technology (IT) related businesses to promote the state as an IT destination. This effort will involve simplifying and rationalising compliances.[28]

We have tried to use elements of **regulatory guillotine framework**[29] and expanding upon the core principles of legality, necessity and business-friendliness[30] In order to expand upon these three principles, we have created a list of indicative questions, where even a minimum of one question will indicate that it is unnecessary/burdensome compliance.[31] This effort will indicate the importance of reducing the compliance burden for digital businesses and general business practices overall. The basis and explanation of each question are given in the box below:

Factors that lead to Potential Unnecessary Compliance Burdens[32]

a. problems with regulations themselves;

Regulations are responsible for unnecessarily increasing compliance burdens in the several ways, some of which are illustrated below:

- Regulatory Uncertainty leads to increasing compliance costs: a lack of clarity provides uncertainty about what is expected of those being regulated and those regulating while increasing the potential for regulators to use their discretion. Regulatory uncertainty acts as a disincentive to invest, as well as potentially increasing compliance costs.
- Excessively prescriptive regulation: prescriptive regulation is typically more complex and onerous than objective- or performance-based regulation, is less flexible, can stifle innovation, and may not allow businesses to deliver the policy outcome at least cost.
- Redundant regulation: regulation may remain in force despite being overtaken by changed circumstances. While providing no benefits, such regulation will still involve compliance costs and could overlap with more recent legislation, causing regulatory confusion.
- Regulatory creep: regulations that influence more areas and activities than were originally intended or warranted. This can stem from the use of subordinate legislation, and regulatory guidelines.

b. poor enforcement and administration; and

- Excessive reporting or recording requirements: requirements beyond the minimum required to enforce a regulation unnecessarily increase compliance costs.
- Regulatory bias or capture: regulators may be 'captured' by particular interests that they deal with on a regular basis, and therefore make decisions favourable to those interests. Such interests could include particular businesses being regulated.

c. unnecessary duplication and inconsistency

Regulatory duplication and inconsistency between jurisdictions are not inherently bad. It may stem from different circumstances between jurisdictions and can lead to better overall outcomes from a competitive federalism perspective. However, duplication and inconsistency can impose some costs:

- Duplication of regulation: the need to provide information to multiple regulators and go through multiple processes can add unnecessarily to compliance costs. For instance, examples might include multiple regulations containing conflicting grievance redressal procedures.
- Inconsistency of regulation: regulatory inconsistencies can occur within or across jurisdictions, and increase regulatory burdens. Inconsistency is likely to present particular problems for businesses operating in multiple jurisdictions.

Is the compliance a part of			
1	Regulatory uncertainty	**Because of problems in regulations themselves**	If yes, then the compliance is unnecessary and burdensome. And needs to be simplified, amended or repealed.
2	Excessively prescriptive regulation		
3	Redundant regulation		
4	Regulatory creep		
5	Excessive reporting or recording requirements	**Because of poor enforcement and administration**	
6	Regulatory bias or capture		
7	Duplication of Regulation	**Leading to unnecessary duplication and inconsistency**	
8	Inconsistency of regulation		

We will thus test potential unnecessary compliances on the list of questions created from the framework mentioned above. If a minimum of one question is answered yes, then deeming the compliance as unnecessary and burdensome. Thus, any unnecessary or burdensome compliance should be amended, simplified, or removed. This will constitute action needed post analysing the compliance through these questions.

In putting the compliances and regulations against these questions, we recommend that the compliances and regulations in their current form are inadequate and need to go through either simplification, amendment or repealment. This paper tries to bring to light various unnecessary compliance requirements and open the discussion about their merits and demerits.

We recognise that all these questions might not be useful for the regulations undertaken analysis in this paper. Still, we include them hoping that this will turn into a framework for regulatory guillotine for other researchers.

Compliance Burdens for Digital Businesses in India

Piyush Goyal, the Minister for Commerce and Industry noted that more than 25,000 compliance requirements have been reduced in the previous exercise of the Centre to promote ease of living and ease of doing business.

Over the years, multiple laws and regulations have been framed for digital businesses and they also prescribe compliances for businesses. However, some compliances are disproportionate and dissimilar to those of traditional businesses. An official statement from the Commerce and Industry ministry stated that technology must aid the initiatives to promote the EoL and EoDB and the system of compliances should not be further complicated.

All businesses, especially in nascent stages, outsource their compliances with regulations to consulting, chartered accountant firms or law firms.[33] Several businesses take the help of consulting firms to create a compliance repository catered to their specific business needs, which is an added cost to the businesses.[34]

These services are called compliance consulting services used by businesses when their specific industry is governed by various complex laws and myriad regulatory agencies. Since navigating so many different laws can be challenging for businesses, compliance consulting services help businesses to make sure that they comply with all these laws.[35]

Below are some rules and regulations that contain cumbersome compliances focused on digital businesses alone.

Information Technology Act, 2000 and Rules thereunder

The Indian Information Technology Act 2000 (IT Act) provides a legal framework for electronic governance by recognising electronic records and digital signatures, defining cybercrimes, and prescribing penalties.[36]

The IT Act is not an all-encompassing legal framework in 'Industry 4.0' age. Though it has gone through one major amendment in 2008, it has not kept pace with the burgeoning growth in the technological sector.[37] Under the IT act, digital businesses are required to follow certain burdensome compliances as follows:

Section 43A and the SPDI Rules Thereunder

Under Section 43A, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) have been prescribed.[38] These rules will be replaced after enacting the draft Data Protection Bill, 2021 (DP Bill, 2021).[39] There are multiple gaps in the rules such as lack of process prescribed in event of data breach and no provisions for collecting and processing of children's data.[40] These issues however are outside the purview of this paper and thus would not be covered.

Section 69 and the 2009 Rules Thereunder

Under Section 69 of the IT act, Intermediaries must provide technical assistance and facilities to secure access, intercept, monitor or decrypt, and provide information stored in computer resources to the central and state government and their agencies. The procedure for the interception, monitoring and decryption is provided in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (2009 rules),[41] which are to be read with Section 69 (2) of the IT act.

Rule 9 of the 2009 rules states that an order for decryption can relate to any information sent to or from a "person or class of persons" or relate to "any subject matter." A decryption request can be issued by one of the ten agencies authorised to intercept communications.[42]

This order was also called the snoop order, which allowed the government to look into the communications of all citizens. The nature of surveillance of this rule and the order authorising ten government agencies to fall into regulatory bias and capture as, if enforced or administered poorly, it causes significant concerns around the right to privacy while increasing the uncertain and apprehensive cost of compliances for digital businesses.[43] This compliance can lead to its potential misuse when assessed on the indicative questions. And its **regulatory uncertainty** makes it possible for unnecessary compliance.

Additionally, Rule 9 allows non-targeted decryption requests that can potentially be directed toward minorities and other vulnerable groups, making for worrisome status due to the country's lack of a surveillance and data protection framework.

Section 69A and the Blocking Rules Thereunder

Under Section 69 A, the GoI had framed the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules)[44] to lay down the rules regarding blocking of information to the public under the IT act as some of the confidential information cannot be disclosed.[45] Under this section, intermediaries can be directed to block public access to any website, internet content, etc., through direction under written orders.

Intermediaries can be directed to block public access to any information or part thereof that is generated, transmitted, received, stored or hosted in any computer resource specified in sub-section (1) of Section 69A of the IT Act. Designated officers can issue such directions[46] under rule 8(6) post a

request for blocking has been received under rule 6 by the nodal officer.[47] However, this examination of requests is often used in a manner that it was not intended to. This was seen in the case of a website called **Dowry Calculator** which was a satirical website made for bringing awareness around the issue of dowry and dowry-related deaths:

Blocking of Dowry Calculator under Blocking Rules

Dowry Calculator was a satirical website that allowed people to calculate how much dowry a man would receive based on his age, caste, profession, salary, alma mater, height, skin colour etc.[48] This when asked to generate results, gave out data on dowry deaths and wrongs associated with dowry while poking fun at patriarchy. In November 2019, the creator of the satirical Dowry Calculator website, Tanul Thakur, filed a writ petition before the Delhi High Court challenging the arbitrary blocking of his website.

In this case, there were multiple reasons for concern around **regulatory bias and capture** due to poor enforcement and administration:

(i) the reasons for blocking the website were not known because the web page merely shows a standard notice stating that, "the URL has been blocked pursuant to the direction of the Department of Telecom. Please contact the administrator for more information".

(ii) MeitY allegedly did not notify the Petitioner before blocking his website because they could not find his contact details, even though the screenshot of the website attached by MeitY displays his name and Twitter handle.[49]

The poor enforcement and administration bringing in **regulatory bias and capture** was also brought to the forefront with a ban on Twitter accounts of farm activists and caravan (a media agency). The accounts were banned by Twitter on a legal demand by MeitY the information of which had to be kept confidential under Rule 16 of the Blocking rules.[50] Regulatory Bias and capture resulting from poor enforcement and administration results in discriminatory treatment of one entity against others without proper reason or with arbitrary action.

Section 70B and the CERT-In Rules Thereunder

Under Section 70B of the IT Act, the GoI had prescribed the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT Rules). On April 28, 2022, the Indian Computer Emergency Response Team (CERT-In) issued new directions (2022 Directions).[51]

CERT Rules only required reporting within a reasonable time frame for cyber-security incidents, the 2022 Directions make this requirement more stringent. Cyber security incidents are now required to be reported within six hours of noticing or being brought to notice of such incidents to the CERT-In.[52] This time frame is insufficient as it would require organisations to reassess their practices and procedures in relation to breach reporting and ensure that appropriate organisational capabilities are deployed to identify and report cyber security incidents in this time frame.[53] This places a burden on businesses for **excessive reporting and recording requirements.**

The 2022 Directions require all entities to synchronise information technology and communications (ICT) system clocks to the Network Time Protocol (NTP) of the National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with other NTP servers traceable to those maintained by NIC or NPL. While global entities are permitted to use a different time source that is in sync with the NTP, they need to ensure that their time source shall not deviate from NPL and NIC.[54] But this requirement has received strong pushback from cybersecurity experts for lacking clarity and being impractical.[55]

The process of synchronisation is complex for multinational organisations that coordinate time across many geographies.

The requirements for synchronised system clocks are also used in the financial sector, trading, and contemporary countries to match the log files with data from all systems.[56] Though time synchronisation is important, various industry experts have highlighted the issues relating to this direction.

There are issues relating to latency where a data centre running with more than the usual number of systems in one place is more likely to bank upon a time server near them and in their control instead of the one provided for by any other party which NIC or NTP approve.[57] To comply with these directions, as non-compliance comes with hefty fines and jail time, businesses small and large will have to dedicate resources for such compliance.

The 2022 Directions require using NIC 's NTP servers. The businesses are still unaware and would be required to find the server configuration, the amount of latency, NIC's NTP servers list, among other security concerns privacy. This would be an **excessive reporting and recording requirement,** to compensate for the latency issue along with the directions being one of the **excessively prescriptive regulations**. The rules were prepared to coordinate action during cyber security emergencies, provide incident response services to users, publish alerts concerning vulnerabilities and threats, and offer information to help improve cyber security.[58] The issued directions do not do any of these things but instead take part in the business strategies of stakeholders, verging into some **regulatory creep.**

Having a single server might be a bad idea.

A technology Generalist remarked to a leading news agency that forcing the entire country in addition to MNCs in other countries to sync with only two-time sources is "a very bad idea."

"It makes those servers a high-value target for cyberattacks. So, the servers will need to be both secure and reliable. But the govt has an abysmal track record on both security and uptime. He adds that the organisational infrastructure can be abused for NTP amplification attacks simply because no business can afford to block traffic from those NTP servers or IP addresses only adds to the problem.[59]

Recently, eleven industry bodies from countries in the European Union, UK, and the US, including the likes of US Chamber of Commerce and US-India Business Council, have written to the CERT-In, arguing that the "onerous nature" of the directive may make it more difficult for companies to do business in India.[60] The CERT rules and the 2022 Directions have multiple other concerns, particularly on data storage mandates that will be discussed in our subsequent discussion paper on cross-border data flow.

Section 87 and the Intermediary Rules Thereunder

Under Section 87 of the IT Act, the Central Government has been given rule-making powers. In utilising these powers and replacing the 2011 Intermediary guidelines, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Rules) were prescribed.[61]

Under the Intermediary Rules, one part focuses on due diligence and grievance redressal by Intermediaries. Another focuses on code of ethics and procedure and safeguards about digital media. All intermediaries are expected to conduct due diligence of the users and content posted on the platforms concerned.[62] Recently, MeitY issued and withdrew amendments to the Intermediary rules in a span of few hours. This is one of the few examples of **regulatory uncertainty** which leads to businesses second-guess the regulatory environment of the country.[63]

Under Rule 3(2) and Rule 11(2) (a), which talk about the grievance redressal mechanism of the intermediary and publisher[64] respectively, states that they should appoint a grievance officer who shall acknowledge the complaint within twenty-four hours and dispose of the complaint in 15 days. The acknowledgement period of twenty-four hours and the 15-day response period is **inconsistent with other regulations** and public systems practices for grievance redressal. For instance, Consumer Protection (E-Commerce) Rules, 2020[65] (E-Commerce Rules 2020) under rule 4 state that the grievance officer shall acknowledge the receipt of any customer complaint within forty-eight hours and redress the same in one month (30 days) time.[66] There needs to be a sync in regulations all across.

Double Standards for Government and its Agencies?

It is noteworthy that the public grievance mechanism for central government, departments and organisations prescribes a prompt and effective grievance redressal mechanism. To ensure this, it is prescribed that grievances should be necessarily acknowledged, with an interim reply within 3 days of receipt and redressed within three months of receipt in the Organisation.[67]

Under Rule 4 (1) a significant social media intermediary (SSMI) is required to comply with specific compliances. These intermediaries include businesses such as search engines, internet service providers (ISPs), digital platforms, etc.[68]

Under Rule 4(1)(a) a, SSMI must appoint a chief compliance officer (CCO), who is required to be a resident of India. The chief compliance officer is responsible for ensuring compliance with the IT Act and Rules.[69]

Significant Social Media Intermediary (SSMI) threshold in India is Inadequate

SSMI has several registered users as notified by the central government, which was later clarified to be at 50 lakh users.[70]

Principle 14 of the UN Guiding Principles on Business and Human Rights, emphasises that the "means through which a business enterprise meets its responsibility to respect human rights will be proportional to, among other factors, its size."[71]

This threshold would have been a step in the right direction if it was not inadequate to calculate this user threshold. Similar was the case of the NetzDG in Germany, which is applicable to intermediaries with 2 million registered users where 88 percent of the population (out of a total of 83.1 million) or 73 million people use the internet. The notification just like the one in India failed to state whether the calculation would be based on active or registered users.

Thus, the German government's threshold is 2.7% of the digital population. Whereas, with approximately 776 million in India, the threshold is 5 million, less than 0.007% of the Indian digital population. Though there is a huge difference in German and Indian digital population, however, as the Indian population is huge in number it is fairly easier for businesses to attain the SSMI threshold in registered users. Therefore, setting such a low threshold might create additional hurdles for smaller social media intermediaries while disincentivizing growth in smaller social media intermediaries.[72]

Thus, for a country with a large demographic like India, the threshold needs to be much higher and there needs to be a clear distinction between active and registered users.

Also, the CCO is required to be a key managerial person of the company or such other senior employee, which can be the CEO or the MD, Chief Financial Officer (CFO), Manager, Company Secretary or Whole-Time Director resident in India.[73] The appointment of the CCO was not without its troubles. The businesses were sceptical about the liabilities attached to the role.[74] This takes away the freedom of the businesses due to it being an excessively prescriptive regulation and comes under the light of **regulatory creep** as the rules intended to create guidelines for intermediaries are creeping into appointments undertaken by the same intermediaries.

Signal is run by a non-profit entity and it may not be possible for such an entity to establish offices or have dedicated personnel in the country.

Under 4(1)(b), the SSMI must appoint a 'nodal contact officer' other than the CCO for 24x7 co-ordination with law enforcement agencies, which must be a resident of India. There are two main issues here; firstly, the law mandates the nodal contact officer to be

different from the CCO, which places an additional cost on SSMI. However, as the threshold for being an SSMI is low in proportion to the population of internet users, it is significantly easier for smaller businesses to be qualified as SSMIs with insufficient resources to meet such compliances. Further, significant social media intermediary (SSMI) is defined as an intermediary with more than 5 million registered users in India. However, there are many intermediaries which have more than 5 million registered users but the number of active users is far lesser. Moreover, there are platforms which offer once-in-a-lifetime service like matrimonial and property buying-selling websites which are not social media per se, and consider the number of inactive users as a mark of their success may also be required to comply with the mandate.[75]

Secondly, there needs to be a 24x7 coordination which would entail more than one nodal contact officer also required to be resident in India as it would not be possible to have a 24-hour employee. It can be understood that 24x7 here means as and when required; however, as the non-compliance of these rules takes away the protection of safe harbour provisions[7677] under Section 79 of IT Act, it is possible for businesses to over-comply by way of more than one employee.

The mandatory requirement can create hurdles for online messaging platforms like Signal or Telegram that do not have offices in India. Similarly, for numerous other intermediaries that operate at a limited scale but meet the threshold of 5 million registered users and can be termed SSMI, this requirement will create an additional financial and operational burden.[78]

Rule 4(2) the rules include an obligation on a significant social media intermediary, primarily messaging services, to identify the first originator of the information on their service when required either by a government (under Section 69 of the IT Act) or court order.

This obligation can only be fulfilled if messaging services technically modify their platform to remove end-to-end encryption or add additional metadata to each message in a way that undermines the security and privacy guarantees that end-to-end encryption offers.[79]

The collateral damage here is citizen's free speech and privacy, which will be unconstitutionally hampered as a result.

Are the Intermediary Rules a repugnant Regulation?

It is a well-settled principle of interpretation of statutes that conferment of rule-making power by an Act does not enable the rule-making authority to make a rule that travels beyond the scope of the enabling Act or is inconsistent or repugnant thereto.[80]

A combined reading of Section 79(2)[81] read with Section 89(2) (zg)[82] makes it clear that the power of the Central Government is limited to prescribing guidelines related to the due diligence to be observed by the intermediaries while discharging its duties under the IT Act. However, the 2021 guidelines have imposed additional requirements and widened the ambit of requirements to be fulfilled by the intermediary.[83]

The Intermediary rules are subordinate legislation under the parent legislation of IT Act and as they exceed the scope of their parent legislation, they move towards **regulatory creep.** It is understood that there is nothing in Section 79 of the IT Act to suggest that the legislature intended to empower the government to mandate changes to the technical architecture of services.[84]

Many platforms (WhatsApp, Signal etc.) retain minimal user data and use E2E encryption to provide privacy to users. Technical experts say that compliance with this requirement is not possible unless end-to-end encryption on messaging services such as WhatsApp is broken.[85] There is a reasonable concern that the compliance requirements will not only break end-to-end encryption but also will lock out platforms that deploy encryption but do not have sizable resources like WhatsApp or Facebook as the businesses will need to rework their model to ensure compliance.[86] For instance, many Indians use Signal and Telegram and these companies will not be able to operate in India in active compliance with these conditions.[87]

What has WhatsApp Argued against the Rules?

WhatsApp has filed a petition in the Supreme Court against the Intermediary rules challenging their constitutionality. Their petition argued that the digital businesses that offer end-to-end encryption would need to rework their model to ensure compliance. These conditions also created a technical requirement for standard encryption practices and deployed protocols. Thereby, it will require the development of new encryption frameworks, which take a long time and degree of peer review to fulfil all cybersecurity norms.[88]

Consumer Protection Act, 2019 and the E-Commerce Rules, 2020 thereunder

The inadequacy of the Consumer Protection Act, 1986 and other associated laws has surged the insecurity and lack of trust among online customers. Therefore, the Consumer Protection Act, 2019[89] replaced the Consumer Protection Act 1986 and became effective on July 20, 2020, while on July 07, 2020, E-commerce Rules 2020[90] came into force to address the e-commerce challenges.[91] The E-commerce rules 2020 are currently under revision due to several government and business concerns.

The proposed amendments to the E-commerce Rules 2020 infringe upon other ministries' mandates and are **inconsistent with regulations** otherwise in place. For instance, the clause for 'fallback liability', which holds platforms liable for mis-selling by third-party sellers is inconsistent with the Finance Ministry's Foreign Direct Investment (FDI) Rules. The FDI Rules prevent platforms from explicitly managing their inventory.[92] For instance, the guidelines for FDI prevent any investment in inventory-based model for e-commerce which means that e-commerce entity will not exercise ownership or control over the goods being sold i.e., inventory.[93]

The Ministry of Corporate Affairs remarked that rules related to the abuse of competitive position are unnecessary since there is already a robust Competition Commission that oversees such issues,[94] thus making it a **regulatory creep** or overreach.

Sensitising Small Sellers Towards Policy

As the rules are still under revision, CUTS CIRC released a research study survey of small sellers who sell goods on Amazon, Flipkart etc. The survey found that 71 percent of these sellers were unaware of any government policy regulating the e-commerce sector. "This indicates a need to sensitise small sellers about e-commerce onboarding and the e-commerce policies in India and their rights."[95]

Dr. Mayaram, Former IAS and Chairman, CIRC, suggested that e-commerce policy must be developmental in approach. This means it should promote the growth of e-commerce by the ease of entry, ease of doing business, and reducing the compliance burden. Regulations have to be light-touch, much like they were for the IT sector back in the 1990s that helped the sector flourish. There should be ease of failure as well in e-commerce.[96]

As per information provided by an officer to a news platform, The Department of Consumer Affairs is bringing in revised e-commerce rules that will also press for "algorithmic fairness" on these marketplaces to remove the advantage that many of these entities give to sellers wholly or partially owned by them and provide a level playing field for small businesses.[97] The nature of the compliance with these rules remains to be assessed.

Payments and Settlement Systems Act, 2007

The Payments and Settlement Act, 2007[98] (PSSA) provides for the regulation and supervision of payment systems in India and designates the RBI as the authority for that purpose. To carry out the provisions of PSSA, RBI is empowered to make regulations by way of circulars.

To adhere to the scope of our study, we will focus on circulars that directly impact digital businesses.

Payment aggregators existing as on March 17, 2020 are required to achieve a net-worth of INR 15 crore by March 31, 2021, and a net-worth of INR 25 crore on or before March 31, 2023, which must be maintained at all times thereafter.

RBI Guidelines for Payment Aggregators and Payment Gateways, 2020

Under the Guidelines for Payment Aggregators (PA) and Payment Gateways (PG), 2020 (2020 Guidelines) issued on March 17, 2020, applicable to entities that facilitate e-commerce sites and merchants in payments termed as Payment Aggregators and entities that provide technology infrastructure for online payments termed as Payment Gateways.[99] On March 31, 2021, RBI made certain clarifications on the 2020 guidelines.[100] (2021 Clarifications)

The 2021 Guidelines state under Clause 6.1 that PA needs to check Payment Card Industry-Data Security Standard (PCI-DSS) and Payment Application-Data Security Standard (PA-DSS) compliance of the infrastructure of the merchants on-boarded. In contrast, clause 6.2 states that Merchants are not allowed to store payment data irrespective of whether they are PCI-DSS compliant. They shall, however, be allowed to store limited data for transaction tracking, for which the required limited information may be stored in compliance with the applicable standards.

There appears to be **regulatory inconsistency** and a contradiction in the clause in 6.1 and 6.2. It is uncertain why merchants would be required to undertake PCI-DSS and PA-DSS compliance if they are not permitted to save any card-related data other than limited data for transaction tracking.

Further, the requirement to comply with PCI-DSS and PA-DSS may be onerous and a **redundant regulation** on small businesses such as sole proprietorships and MSMEs and will impede their operations and ability to use online payment modes on account of such restrictions.[101]

The 2021 clarifications do not change the requirement of background checks[102] of merchants by PAs. These requirements have certain underlying **regulatory uncertainties,** such as, whereby a merchant may use the payment aggregator's services solely to collect payments from its customers. In contrast, the actual transactions with respect to delivery of goods or provision of services would be conducted offline.[103]

Also, undertaking background checks for merchants who sell their goods or services offline and do not have a website would not be a commercially feasible process. The 2020 Guidelines also impose the obligation on PAs to check their merchants to verify whether appropriate terms and conditions have been uploaded on the merchant website. The Guidelines do not address instances where a merchant may not have its website or may have availed listing services provided by third parties and, therefore, will be unable to display terms and conditions. This requirement is not feasible and would be difficult for a payment aggregator to comply with.[104]

Can obtaining a PA licence be more complicated?

At least 185 fintech firms with ambitions to be non-bank payment providers have placed applications to become licensed PAs. It was allegedly reported that RBI has decided to reject the payment aggregator licence of ZaakPay, which runs MobiKwik. Its crypto partnerships and failure to meet the laid-down net-worth criterion are some of the reasons for the rejection.[105]

This might have been done under the checking of 'fit and proper' status of the applicant entity and management by obtaining inputs from other regulators, government departments, etc., as deemed fit.[106]

The RBI, during its due diligence will also check on aspects related to what percentage of the business revenue comes from unregulated entities such as online betting or crypto exchanges. It will also evaluate money-laundering concerns and whether these aggregators are compliant with its tokenisation norms.[107]

RBI has said that to protect consumer's interest, all past dealings of applicants for PA licence will be in question without a chance of negotiation.[108] The delay in the licence process is a likely reason for **regulatory uncertainty**.

RBI Circular for Processing of E-Mandates, 2019

The World Bank has identified 'payments' an important digital business indicator[109] that is central to digital business activities. In August 2019, RBI issued a circular[110] on the processing of e-mandates on cards for recurring transactions to balance the safety and security of card transactions with customer convenience. The circular is applicable to debit and credit cards and Unified Payments Interface (UPI) but not on net banking. The initial deadline to comply with the circular was March 31, 2021. Still, the RBI had to extend it to September 30, 2021, as the stakeholders expressed their inability to meet the compliance.

The E-mandate though with additional time given for compliance has caused massive disruption after the deadline as consumers set up their fresh mandates. Allegedly, many businesses on their platform lost out on subscribers since users did not want to take the effort of manually making payments every month.[111]

Smaller Businesses are Hit Worse

Leap Club, a monthly subscription-based professional network for women, lost 10 percent of its subscribers in the first few months after the RBI's new recurring payment guidelines came into effect. Its owner remarked that, 'while 10 percent is a small share, it is surely a big hit for small businesses' revenues.'

The platform has now moved from monthly subscriptions to yearly subscriptions to cut out the surmounting work behind reminding customers to make manual payments every month. But that comes with its share of challenges while onboarding new customers.

"People think a lot more before making any annual subscriptions, and they usually want to try the product for a month or two, but that is not possible now," the platform owner remarked. Six months after the deadline, many small businesses still do not have the option to set up recurring payments on our debit and credit cards. Back-end efforts to make these payments manually to avoid disruptions in day-to-day operations have substantially increased.[112]

Similar issues are being faced by donation platforms and non-governmental organisations which work on periodic donations.

Under the E-mandate guidelines for auto-debit without additional factor authentication, many digital businesses stopped supporting India-issued cards to avoid **complex regulation** and underlying compliances.

First Heroku, now Apple and Many more in Between

Heroku, a cloud platform as a service (PaaS) stopped verifying and processing India-issued credit cards for Heroku Online customers due to the new RBI regulations stating that they can no longer process automatic recurring payments using India-issued credit cards without an additional factor of authentication.[113]

Apple has stopped accepting card payments for subscriptions and app payments on the App Store. Users in India can no longer use their credit or debit cards to make payments for services or purchases on the App Store. The Apple Support page shows that users can purchase and subscribe to services by paying through net banking, UPI or Apple ID Balance.[114]

The Draft Data Protection Bill, 2021

After extensive consultations, the Joint Parliamentary Committee (JPC) submitted its report in December 2021, including recommendations and the Draft Data Protection Bill, 2021 (DP Bill).[115] There are talks that completely new legislation may replace the current proposed law. However, the bill in its current form with its compliance requirements will cripple the industry allegedly.[116]

However, even before it becomes a law, the businesses and people under its jurisdiction have started to worry about the set of compliances that will come with it. The DP Bill has undertaken **regulatory creep** as the scope of DP Bill, though earlier limited to personal data, has now been expanded to non-personal data (NPD). The small businesses that do not deal in personal data but provide services and infrastructure might have to gear up to comply with the bill's NPD requirements.[117] The NPD requirements would entail reporting of data breaches of personal as well as non-personal data, along with businesses having to give the users option to opt out of data anonymisation. A leading online gig platform representative in a panel for NPD remarked that start-ups would have to spend resources to manage information, have separate dataset tools where certain data cannot be used for business purposes, or data that can be used for public good purposes or that which is important to the government.[118]

More difficult for Start-ups

A representative of Zeta (a fintech startup), said the DP Bill as a law in its current form is 'compliance heavy'. And that "the real teeth of this law will be shown in the regulations and codes of practice issued on things like privacy by design, the right to be forgotten, and more. Until those regulations come up, you are operating in a nebulous space, where you're making educated guesses on the basis of European experiences like the GDPR." He believed that newer data-centric start-ups would find it difficult to enter the market and expand when the law comes into force.[119]

The DP bill in itself is cause for **regulatory uncertainty** as firstly, the current legislation might allegedly be replaced with new legislation, and secondly, the timeline of the bill becoming a law is still uncertain. However, even if the bill becomes a law, much of the processes of the law has been left for future regulators (Data Protection Authority (DPA)) to determine. This will lead to many compliance-related requirements unclear for digital businesses, including how NPD might be regulated.[120] NPD's other compliances regarding data sharing and storage will be covered in our subsequent paper on data localisation.

It has been debated that the full effect of the compliance burdens will be seen only after its implementation, however, it will have an increased compliance burden on start-ups[121] that build products for children specifically.[122] Indian companies that function in edtech, online gaming and social media services for children will have to deal with additional compliance requirements. These compliances stem

from the provisions of age verification and consent, which treat all under the age of 18 years with a single lens[123], thus leading to major compliance burdens for large and small enterprises.[124]

Disincentivising Start Ups?

The bill puts a blanket ban on profiling children, making customisation of services difficult, such as using artificial intelligence for offering customised programmes for children in a classroom as per their learning abilities, which might disincentivize innovation for this target group.[125]

In recent times, investors have backed start-ups across a range of sectors - fintech, software as a service (SaaS), ecommerce, travel, healthcare, and education - many of which have become unicorns. However, by imposing such requirements, there is a risk for Indian start-ups to register outside India to avoid onerous compliance. Therefore, there is a possibility of undoing decades of the progress in the Indian startup ecosystem, by implementing the current data protection framework.[126]

Miscellaneous Unnecessary Compliances

Though the paper has covered major regulations and their compliance requirements above, certain provisions across these regulations fall under the radar of being unnecessary because they are a part of **excessive reporting or recording requirements**, **duplication of regulation, or inconsistency of regulation** with each other. Due to these, they often remain a redundant regulation that, though not required, still incurs compliance costs. This section will deal with provisions that contain similar provisions or provisions for similar purposes with different processes for similar kinds of businesses.

Appointments

Under various regulations and laws, there has been a requirement to appoint nodal officers, grievance officers, and others that have the same function.

For instance, the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (Traffic Data Rules), Rule 4(3) intermediaries must designate one or more officers,[127] who are required to receive and handle requisitions from the nodal officers of the competent authority ("Monitoring requisitions") for monitoring/collecting traffic data.

Do five or more different regulations and laws need to prescribe the appointment of an officer or grievance redressal officer for one similar business type?

Similarly, under Blocking Rules, rule 13 an intermediary need to appoint an appropriate person to receive and handle the directions for blocking public access to the information in electronic format. Also, under SPDI Rules (to be replaced with DP Bill), under rule 5(9) the intermediaries must designate a grievance officer and publish his name and contact information on the website.

Further, under Intermediary rules, rule3(2) an intermediary shall appoint a grievance officer responsible for dealing with the grievances in a prescribed manner. Also, the Draft DP Bill calls for a Data Protection Officer (DPO) who needs to be a key managerial person. These regulations are duplicated as they deal with handling requisitions, directions, and grievances.

Acknowledgement, Reporting and Recording Requirements

Under Traffic Data Rules, Rule 4(8), the designated officer of the intermediary must acknowledge the receipt of monitoring requisitions within 2 hours from the time of receipt. Further, the designated officer must forward a list of Monitoring requisitions to the relevant nodal officer every 15 days.

Further, under the newly amended CERT Rules, every event which may fall into the ambit of 'cyber incident' will need to be reported within six hours of becoming aware of such events.[128]Also, under the Blocking Rules, rule 13(2) designated officers must acknowledge directions received within two hours through an acknowledgment letter or email with an e-sign.

International Standards of Timeline more Desired

11 industry bodies have written to the Indian Computer Emergency response Team in light of the recent CERT Rules' amendment. In their letter, they stated that the 'cybersecurity directive will have a "detrimental impact on cybersecurity for organisations that operate in India, and create a disjointed approach to cybersecurity across jurisdictions, undermining the security posture of India and its allies in the Quad countries, Europe, and beyond.'

A 6-hour timeline is unnecessarily brief and injects additional complexity at a time when entities are more appropriately focused on the difficult task of understanding, responding to, and remediating a cyber incident.[129]

Intermediary rules Under Rule 3(2) the grievance officer appointed by the intermediary shall acknowledge the complaint within 24 hours and dispose of the complaint in 15 days. Also, in the DP bill, any data breach, including NPD, has to be reported within 72 hours of becoming aware of such a breach.[130]

Way Forward

In all the ways that unnecessary compliances impact businesses, digital businesses, especially start-ups and small businesses are hit twice as hard. The cost of regulations is a burden on the resources of the businesses and all unnecessary and disproportionate compliance must be minimised. Regulations are in place to support businesses and consumers; however, unnecessary red tape will hinder businesses from using resources productively and innovatively.

Moreover, the efforts and costs that firms spend to comply with unnecessary aspects of any regulatory regime can impede a firm's ability to meet its business performance goals.[131] To reduce the cost of compliance and the burden of regulations from digital businesses, we propose the following points of deliberation:

Simplify, Amend or Repeal

Based on the above-identified unnecessary compliances and the regulatory guillotine, compliances focused on digital businesses should be simplified, amended and repealed as per the suitability of each regulatory guillotine indicator. For instance, compliances relating to the appointment of grievance redressal officers or designating officers for handing requisitions and directions can be taken away from multiple regulations and placed in one place. Thus, reducing the number of compliances by clubbing of same or similar compliances.

Regulatory experts say our complex rules induce small firms to remain small./ It's compliance burden and not high interest or tax rates choking smaller business entities. The more complex the regulations and compliance requirements, the greater is the disadvantage of small business entities which do not have dedicated regulatory affairs teams or financial muscle to deal with them.[132]

To simplify, amend and repeal the unnecessary compliances, GoI can take the various steps, some of which though already existent, need to be tailored for digital businesses alone. These steps can include:

a. Making a Central Repository for Compliances

In January 2021, the Department for Promotion of Industry and Internal Trade (DPIIT) s launched the Regulatory Compliance Portal to monitor the sector-wise reduction in compliance burden. This was done to acknowledge that compliance and regulatory scrutiny are among the biggest challenges our country faces in the Ease of Doing Business.[133]

There are multiple laws and regulations in the country to cater to digital businesses. Several businesses use consulting firms' help to create a compliance repository catered to their specific business needs,

which is an added cost to the businesses.[134] This qualifies as a service which newer businesses and nascent stage start-ups would not be able to afford or budget for.[135]

A not-so-novel solution to increased compliances and regulations which mirror other regulations creating the chances of over-compliances is to have a government-led central repository of compliances for specifically digital businesses as a subset of the larger compliance portal.

What the Repository can look like?

Under this repository, all laws and compliances will be listed down so businesses can filter the repository based on the nature of business, size, operations, employees, etc. This filterable repository will enable businesses to look at duplicitous compliances, overlap, or already required to be fulfilled otherwise. This will also enable the government to understand the regulatory overlap and create a standardised list of compliances for businesses. The government will then be able to do away with duplicate compliances and create a more cohesive regulatory environment.

Most of this is being done about the Regulatory Compliance Repository and needs to be replicated for digital business compliances.

This will also be in line with the simplification of compliances and elimination of compliances, which will have a transformative impact and multiplier effect on EoDDB.[136]

b. Use of Technology for reducing compliances and costs associated with them

The age of digitalisation has advanced to make things simpler for consumers. Similar thoughts should be used while dealing with compliances. Digital Businesses must use resources to track new regulatory events, determine how relevant each event is to the business, and then decide whether there are changes that need to be made to policies and procedures.[137]

Regulation Technology (RegTech) is used to ease compliances and their burden on digital businesses. One such example is financial services. Over the recent past, hundreds of start-ups have begun to apply digital technology to the now numerous and burdensome tasks required to comply with regulations. RegTech promises to cut the cost of compliance processes and improve effectiveness to make them quicker and more reliable, reduce hassle for customers, and reduce the risk of costly compliance failures.[138]

Use of Technology for compliance supports and promotes holistic digital compliance, including data integration, verification and visualisation. Demand for integrated, utility-based risk management and reporting covers various regulations across financial and non-financial risks.[139] RegTech helps simplify, streamline, and automate the regulatory compliance processes of your business, and it can help you reduce the risk of fines, penalties, and legal implications. This technology helps companies stay in compliance, protect consumers and regulators, and provide a smooth transition for innovation.[140] For instance, global firms have been moving towards deploying RegTech for regulators where the teams partner with leading authorities to come up with robust mechanisms for Supervision Technology (SupTech)[141]

Institutionalising Regulatory Impact Assessment

Regulations have widespread impacts and affect multiple stakeholder groups in different ways. A sub-optimal regulation is most likely to increase the cost of administration and compliance, have unintended outcomes and limit the likelihood of achieving its objectives. Therefore, it is of paramount importance to understand the impacts of any regulation, proposed or in operation, to achieve favourable outcomes.

Regulatory Impact Assessment (RIA) systematically identifies and assesses direct and indirect impacts of regulatory proposals and existing regulations, using consistent analytical methods. It involves a participatory approach via a public consultation to assess such impact, determine costs and benefits,

and select the most appropriate regulatory alternative.[142] RIA should be used to evaluate both existing and proposed legislation through the regulation-making process for its use of regulations on the indicators of cost, time spent, and human resources deployed, among others.

The New Zealand Way

Recently, the Prime Minister of New Zealand in response to concerns about specific regulatory imposts for which there seemed to be inadequate justification, invited members of a public initiative body to provide a list of regulations that they considered needed to be modified or scrapped. This allowed varied opinions and rationales to become part of the regulatory process and lead to more generally regulatory quality and practice.[143]

This is one of the many ways to rationalise compliances. The policymakers must use the process of crowdsourcing to find details of compliances that are cumbersome and work towards rationalising them.[144]

In this regard, CUTS had undertaken research on institutionalising RIA in India. Under said research, it was established that RIA should be adopted by legislation mandating its adoption. Also, the briefing paper suggested that there should be dedicated RIA Units within all government departments and regulatory agencies.[145] For instance, each department has a Better Regulation Unit (BRU), which oversees the department's processes for better regulation and advises on how to comply with the requirements. The BRU works with government departments to monitor the measurement of regulatory burdens, coordinate their reduction, and ensure that the regulation remains smarter, better targeted, and less costly to business.[146]

On these lines in a previous study on RIA, CUTS had recommended creation of a Regulatory Productivity Commission (RPC) at the Centre and states. The RPC would be able to supervise RIA process and act as an independent reviewer of RIA statements.[147]

One In One Out (OIOO)

This concept had been implemented in the United Kingdom, however, after Britain's exit from the European Union, the same was removed from practice. However, we feel there is merit in the system. OIOO and the red-tape challenge have helped the UK to reduce the annual cost to business of domestic regulations by almost $2.2 billion ($10 billion cumulatively). OIOO mandated that if any government department in the UK wanted to bring in new regulation (which was not part of the party manifesto), the department would have to find ways to remove one time the Compliance Cost.[148]

UKs Coalition government while introducing OIOO: "We will cut red tape by introducing a 'one-in, one-out' rule whereby no new regulation is brought in without other regulation being cut by a greater amount."

To manoeuvre the OIOO system for India, we suggest that each time any regulator or the government introduces new compliance, compliances should be able to replace at least one existing compliance not only in number but more so in the cost imposed by said compliances. As the intent of all regulations is to create a business-enabling environment, then new regulations must better the existing situation. The OIOO regulation checker will allow for better regulation and reduction of red tape to a greater extent.

Endnotes

[1] 'Digital economy to see exponential growth to US$800 bn by 2030: FM', March 31, 2022, The Economic Times, *available at* Digital economy to see exponential growth to $800 bn by 2030: FM - The Economic Times

[2] Rampal, Nikhil, ''Process is punishment; govt loves paper': MSMEs call out unease of doing business in India', 10 September 2021, The Print, *available at* 'Process is punishment, govt loves paper': MSMEs call out unease of doing business in India.

[3] Sarkar, Shankhyaneel, 'Centre introduces measures to reduce 'compliance burden' to increase ease of doing business', 28 September 2021, Hindustan Times, *available at* Centre introduces measures to reduce 'compliance burden' to increase ease of doing business - Hindustan Times

[4] Corvello, Vincenzo, Verteramo, Severino, et al, 'Thrive during a crisis: the role of digital technologies in fostering antifragility in small and medium-sized enterprises', 22 March 2022, Journal of Ambient Intell Human Comput, *available at* Thrive during a crisis: the role of digital technologies in fostering antifragility in small and medium-sized enterprises | SpringerLink

[5] 'Consumer sentiment and behaviour continue to reflect the uncertainty of the COVID-19 crisis', 26 October 2020, McKinsey and Company, *available at* Consumer sentiment and behaviour continue to reflect the uncertainty of the COVID-19 crisis.

[6] Alawadhi, Neha, 'India's consumer digital economy to grow 10x to $800 bn by 2030: Redseer', 1 July 2021, Business Standard, *available at* India's consumer digital economy to grow 10x to $800 bn by 2030: Redseer | Business Standard News

[7] 'India's trillion-dollar digital opportunity' *available at* India's Trillion Dollar Digital Opportunity

[8] *Ibid*.

[9] 'Ease of doing business: India jumps 30 notches, breaks into top 100', 31 October 2017, The Times of India, *available at* Ease of doing business: India jumps 30 notches, breaks into top 100

[10] 'India's trillion-dollar digital opportunity' *available at* India's Trillion Dollar Digital Opportunity

[11] Subramaniyan, Dr. Chandrika, 'Why India must amend its Information Technology Act in the age of Artificial Intelligence' 2019, IEEE India Info. Vol. 14 No. 4, *available at* Why India must amend its Information Technology Act in the Age of Artificial Intelligence

[12] Press Release, Ministry of Commerce and Industry, 28 September 2021, *available at* https://pib.gov.in/PressReleasePage.aspx?PRID=1758949

[13] Cole, Ben, 'Regulatory Compliance', *available at* What is regulatory compliance?

[14] Chikermane, Gautam and Agarwal, Rishi, 'Jailed for Doing Business: The 26,134 Imprisonment Clauses in India's Business Laws', February 2022, Observer Research Foundation, *available at* https://www.orfonline.org/wp-content/uploads/2022/02/ORF_Monograph_JailedForDoingBusiness_Final-New-11Feb.pdf

[15] Chikermane, Gautam and Agarwal, Rishi, 'Jailed for Doing Business: The 26,134 Imprisonment Clauses in India's Business Laws', February 2022, Observer Research Foundation, *available at* https://www.orfonline.org/wp-content/uploads/2022/02/ORF_Monograph_JailedForDoingBusiness_Final-New-11Feb.pdf

[16] Grilo, I. and A.R. Thurik (2008), Determinants of entrepreneurial engagement levels in Europe and the US, Industrial and Corporate Change, *available at* Determinants of Entrepreneurial Engagement Levels in Europe and the Us | Request PDF

[17] Howells, G. Protecting Consumer Protection Values in the Fourth Industrial Revolution. J Consum Policy 43, 145–175 (2020). *available at* https://doi.org/10.1007/s10603-019-09430-3

[18] 'Compliance brings international consequences for digital business', ZDNET, *available at* Compliance brings international consequences for digital business | ZDNet

[19] Hammond, Sussanah and Cowan, Mike, 'Cost of Compliance: New Decade, New Challenges, 2020, Thomson Reuters, *available at* the cost of Compliance Report 2020 and Covid-19 Update

[20] Sarkar, Shankhyaneel, 'Centre introduces measures to reduce 'compliance burden' to increase ease of doing business', 28 September 2021, Hindustan Times, *available at* 'Centre introduces measures to reduce 'compliance burden' to increase ease of doing business - Hindustan Times

[21] Bhat, Prashant, 'Data Privacy-The new challenge on the compliance scape in India', 02 May 2022, The Economic Times, *available at* Data Privacy-The new challenge on the compliance scape in India

[22] 'How Will The Proposed Data Protection Law Affect Your Startup?', Inc 42, 15 March 2022, *available at* How Will The Proposed Data Protection Law Affect Your Startup?

[23] 'Making regulation a competitive advantage', Deloitte, 2020 *available at* Making regulation a competitive advantage

[24] What does compliance cost mean?

[25] Kenton Will, 'Compliance Cost', 29 June 2021, Investoppedia, *available at* Compliance Cost Definition

[26] Singh, Ritesh, 'How to help small businesses: Cut heavy costs of regulatory and tax compliance, make credit available', November 21, 2019, The Times of India *available at* How to help small businesses: Cut heavy costs of regulatory and tax compliance, make credit available

[27] 'Indian companies continue to pay a high cost for compliance, report says', 08 July 2020, Money Control, *available at* Indian companies continue to pay a high cost for compliance, report says

[28] 'Goa govt will ensure ease of doing business for start-ups, IT-related businesses for start-ups, IT-related businesses: Minister', 21 April 2022, The Economic Times, *available at* Goa govt will ensure ease of doing business for start-ups, IT-related businesses: Minister

[29] Any regulation that is not justified as legal and necessary for government policy in a market economy will be eliminated. Any regulation that is legal and needed but not business-friendly will be simplified to the extent possible.

[30] 'The Regulatory Guillotine™ Strategy', December 2005, USAID, *available at* The Regulatory Guillotine™ Strategy

[31] Productivity Commission 2009, Review of Regulatory Burden on the Upstream Petroleum (Oil and Gas) Sector, Research Report, Melbourne, *available at* Review of Regulatory Burden on the Upstream Petroleum (Oil and Gas) Sector - Research report

[32] Productivity Commission 2009, Review of Regulatory Burden on the Upstream Petroleum (Oil and Gas) Sector, Research Report, Melbourne, *available at* Review of Regulatory Burden on the Upstream Petroleum (Oil and Gas) Sector - Research report

[33] Through Stakeholder Consultation with Digital Startup.

[34] 6 Reasons Why Businesses Need Compliance Consulting

[35] Vreese, Piet De, 'The rising cost of regulatory compliance for financial institutions', March 2021, Pideeco, *available at* The rising cost of regulatory compliance for financial institutions

[36] Information Technology Act, 2000 *available at* Information Technology Act, 2000

[37] Thomas, K. Sunil, 'Imminent need to strike a balance between digital innovation and right to privacy', 21 October 2020, The Week, *available at* 'Imminent need to strike a balance between digital innovation and right to privacy' - The Week

[38] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, *available at* SPDI Rules.

[39] Schedule of Draft Data protection Bill, 2021.

[40] Thakur, Shanuja, 'Relevance of Sensitive Personal Data Information Rules, 2011 in 2021', 1 November 2021, available at https://blog.ipleaders.in/relevance-of-sensitive-personal-data-information-rules-2011-in-2021/

[41] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, *available at* Procedure and Safeguards for Interception, Monitoring and Decryption

[42] 'MHA authorises 10 central agencies to intercept calls, data on any computer: Mamata, Omar, Owaisi slam move', 21 December 2018, First Post *available at* MHA authorises 10 central agencies to intercept calls, data on any computer: Mamata, Omar, Owaisi slam move- Technology News, Firstpost

[43] Mohanty, Bedvyasa, 'The Encryption Debate in India', 30 May 2019, International Encryption Brief, Carnegie, *available at* The Encryption Debate in India - Carnegie Endowment for International Peace

[44] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, *available at*,Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009

[45] S, Aishwarya, 'Information Technology (Blocking Rules), 2009 and Section 69a of the IT Act, 2000', 22 November 2021, Ipleaders, *available at* Information Technology (Blocking Rules), 2009 and Section 69a of the IT Act, 2000 - iPleaders

[46] Per Rule 3 of the Blocking Rules.

[47] Per Rule 4 of the Blocking Rules.

[48] 'Blocking of satirical dowry calculator website prompts us to take action!' Internet Freedom Foundation *available at* Blocking of satirical dowry calculator website prompts us to take action! #WhatTheBlock #SaveTheInternet

[49] 'MeitY defends blocking of satirical Dowry Calculator website #FreeToMeme', Internet Freedom Foundation, *available at* MeitY defends blocking of satirical Dowry Calculator website #FreeToMeme

[50] Sachdev, Vakasha, 'Is the Ban on Twitter Accounts of Caravan, Farm Activists Legal?', 03 February 2021, The Quint, *available at* Is the Ban on Twitter Accounts of Caravan, Farm Activists Legal?

[51] 'Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.' 28 April 2022 *available at* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[52] *Ibid*.

[53] Sanyal, Jishnu et.al, '2022 CERT-In Directions on Reporting Cyber Incidents', 4 May 2022, Lexology, *available at* 2022 CERT-In Directions on Reporting Cyber Incidents - Lexology

[54] 2022 Directions *available at* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[55] Mathi, Sarvesh, 'Companies Can Use Own Time Source but There's a Caveat', 18 May 2022, Medianama, *available at* https://www.medianama.com/2022/05/223-cybersecurity-directive-time-sync/

[56] Bartels, Randy, 'PCI Requirement 10.4 – Using Time-Synchronization Technology, Synchronize All Critical System Clocks and Times', 1 May 2018, *available at* PCI Requirement 10.4 – Using Time-Synchronization Technology, Synchronize All Critical System Clocks and Times

[57] Mathi, Sarvesh, 'Why India's New Cybersecurity Directive Is a Bad Joke', 5 May 2022, Medianama, *available at* Why India's new cybersecurity directive is a bad joke

[58] CERT Rules, 2014, *available at* Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

[59] Ghosh, Soumik, ' CERT-In's directives on ICT system logs, incident reporting present operational challenges', 19 May 2022, The Economic Times, *available at* cert: CERT-In's directives on ICT system logs, incident reporting present operational challenges, IT Security News, ET CISO

[60] Barik, Soumyarendra, 'Cybersecurity norms may make it 'difficult' to do business in India: 11 industry bodies to CERT-In', 28 May 2022, Indian Express, *available at* https://indianexpress.com/article/business/cybersecurity-norms-may-make-it-difficult-to-do-biz-in-india- 11-industry-bodies-to-cert-in-7940437/

[61] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at Intermediary Rules

[62] 'No social media intermediary can violate constitutional rights of citizens: IT Ministry sources', 29 March 2022, The New Indian Express, *available at* No social media intermediary can violate constitutional rights of citizens: IT Ministry sources

[63] Mundhra, Laxitha, 'MeitY Withdraws IT Rules Amendments Within Hours To 'Make Changes'', 3 June 2022, Inc42, *available at* https://inc42.com/buzz/meity-withdraws-it-rules-amendments-within-hours-to-make-changes/

[64] The Publisher includes Publisher of news and current affairs content and publisher of online Curated content. This would include all websites and platforms that share information, ed-tech platforms, OTT platforms, SSMI which hosts accounts which curate content of all kinds.

[65] E-commerce Rules 2020, *available at* https://consumeraffairs.nic.in/sites/default/files/E%20commerce%20rules.pdf

[66] Rule 4(5), E-commerce Rules 2020.

[67] Grievance Redressal Mechanism in the Government under the Department of Administrative Reforms and Public Grievances Grievance redress mechanism in Government.

[68] How the intermediaries' rules are anti-democratic and unconstitutional.

[69] 'Platforms with over 50 lakh users to be 'significant social media intermediaries', February 28, 2021, The Indian Express, *available at* Platforms with over 50 lakh users to be 'significant social media intermediaries' | Technology News, The Indian Express

[70] 'Govt sets '50 lakh users' threshold to define 'significant social media intermediary' under IT rules', 27 February 2021, The Tribune, *available at* Govt sets '50 lakh users' threshold to define 'significant social media intermediary' under IT rules

[71] Guiding Principles on Business and Human Rights, United Nations Human Rights, 2011, *available at* GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS

[72] Sarkar Torsha et al., 'On the Legality and Constitutionality of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021', 22 June 2021, Medianama, *available at* https://www.medianama.com/2021/06/223-legality-constitutionality-of-it-rules/

[73] Section 2(51) of Companies Act, 2013 gives the definition of Key Managerial Person.

[74] Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, *available at* Fat salary but bigger risks: Is this a tech job that nobody wants?

[75] Matthan, Rahul, 'Digital intermediary rules confuse more than clarify', 26 May 2021, Live Mint, *available at* https://www.livemint.com/opinion/columns/digital-intermediary-rules-confuse-more-than-clarify-11621957664680.html

[76] Sharma, Neelanjana, 'Impact of Criminalising Provisions on Ease of Doing Digital Business in India', March 2022, CUTS CCIER, *available at* https://cuts-ccier.org/pdf/dp-impact-of-criminalising-provisions-on-ease-of-doing-digital-business-in-india.pdf

[77] Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, available at https://www.moneycontrol.com/news/business/economy/fat-salary-but-bigger-risks-is-this-a-tech-job-that-nobody-wants-7128991.html

[78] 'Analysis of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021'. 27 February 2021, SFLC, *available at* Analysis of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

[79] Sarkar Torsha et al., 'On the Legality and Constitutionality of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021', 22 June 2021, Medianama, *available at* https://www.medianama.com/2021/06/223-legality-constitutionality-of-it-rules/

[80] State of Karnataka and Another v. Ganesh Kamath & Ors (1983 SCR (2) 665), *available at* https://indiankanoon.org/doc/1245411/

[81] IT Act 2000.

[82] *Ibid*.

[83] Sarkar Torsha et al., 'On the Legality and Constitutionality of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021', 22 June 2021, Medianama, *available at* https://www.medianama.com/2021/06/223-legality-constitutionality-of-it-rules/

[84] *Ibid*.

[85] Mendiratta, Raghav, 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021', 26 March 2021, Stanford, *available at* Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 | wilmap

[86] B, Nitin, 'How govt's new IT Rules to 'track originator of messages' can affect your privacy', 25 February 2021, The News Minute, *available at* How govt's new IT Rules to 'track originator of messages' can affect your privacy | The News Minute

[87] *Ibid*.

[88] Whatsapp LLC v. Union of India, the petition by whatsapp is *available at* IN THE HIGH COURT OF DELHI AT NEW DELHI (EXTRA ORDINARY CIVIL WRIT JURISDICTION) WP (C) NO. _____ OF 2021 IN THE MATTER OF:

[89] Consumer Protection Act, 2019, *available at* Consumer Protection Act, 2019.

[90] E-commerce Rules, 2020, *available at* E-commerce Rules, 2020.

[91] Chawla, Neelam and Kumar, Basanta, 'E-Commerce and Consumer Protection in India: The Emerging Trend', 09 July 2021, Journal of Business Ethics, *available at* E-Commerce and Consumer Protection in India: The Emerging Trend | SpringerLink

[92] Racherla, Pradeep, 'Draft e-commerce rules: The Good, the Bad, and the Missing', 22 February 2022, The Hindu Business Line, *available at* Draft e-commerce rules: The Good, the Bad, and the Missing - The Hindu BusinessLine

[93] Consolidated FDI Policy effective from 15.10.2020, DPIIT *available at* https://dpiit.gov.in/sites/default/files/FDI-PolicyCircular-2020-29October2020.pdf

[94] Racherla, Pradeep, 'Draft e-commerce rules: The Good, the Bad, and the Missing', 22 February 2022, The Hindu Business Line, *available at* Draft e-commerce rules: The Good, the Bad, and the Missing - The Hindu BusinessLine

[95] Sodhi, G., Agrawal, B., Priya (2022), "Festive Economy and Online Retail for MSMEs in India", CIRC, *available at* https://circ.in/wp-content/uploads/2022/05/Festive-Economy-Report-CIRC.pdf

[96] Soni, Sandeep, 'Several MSME sellers not aware of any govt policy regulating e-commerce in India: Survey', 6 May 2022, *available at* Several MSME sellers not aware of any govt policy regulating e-commerce in India: Survey | The Financial Express

[97] Nair, Sobhana K., 'Govt to tweak rules for e-commerce portals', 20 April 2022, The Hindu, *available at* Govt to tweak rules for e-commerce portals - The Hindu

[98] Payments and Settlement Systems Act, 2007 *available at* Payment and Settlement Systems Act, 2007

[99] Guidelines on Regulation of Payment Aggregators and Payment Gateways, 17 March 2020, *available at* guidelines for regulation of Payment Aggregators (PAs) and Payment Gateways (PGs)

[100] Clarification issued by RBI dated March 31, 2021 *available at* Guidelines on Regulation of Payment Aggregators and Payment Gateways

[101] 'A critique of the payment gateways and payment aggregators guidelines', Spice Route Legal, *available at* A critique of the payment gateways and payment aggregators guidelines - Spiceroutelegal

[102] A background check would include for the PA to ensure that such merchants do not have any malafide intention of duping customers, do not sell fake / counterfeit / prohibited products, etc.

[103] 'A critique of the payment gateways and payment aggregators guidelines', Spice Route Legal, *available at* A critique of the payment gateways and payment aggregators guidelines - Spiceroutelegal

[104] *Ibid*.

[105] Bhalla, Tarush and Shukla, Saloni, 'RBI lens on companies seeking payment aggregator licence', 25 April 2022, The Economic Times, *available at* RBI News: RBI lens on companies seeking payment aggregator licence - The Economic Times

[106] 20201 Guidelines clarifications

[107] Bhalla, Tarush and Shukla, Saloni, 'RBI lens on companies seeking payment aggregator licence', 25 April 2022, The Economic Times, *available at* RBI News: RBI lens on companies seeking payment aggregator licence - The Economic Times

[108] *Ibid*.

[109] Chen, Rong, 'Digital Business Indicators', *available at* Digital Business Indicators

[110] RBI Circular on Processing of E-Mandates for recurring payments, 21 August 2019, *available at* RBI Notification

[111] Iyer, Priyanka, 'RBI guidelines on recurring payments continue to cause disruption even after 6 months of deadline', 25 March 2022, Money Control, *available at* RBI guidelines on recurring payments continue to cause disruption even after 6 months of deadline

[112] *Ibid*.

[113] 'India-Issued Credit Cards Not Accepted for Heroku Online', 15 December 2021, *available at* India-Issued Credit Cards Not Accepted for Heroku Online

[114] 'RBI rules break Apple payments in India, Apple stops taking credit and debit card payments', 6 May 2022, India Today, *available at* RBI rules break Apple payments in India, Apple stops taking credit and debit card payments - Technology News

[115] JPC Report on Personal Data Protection Bill 2019 and the Draft Data Protection Bill, 2021 *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[116] Agarwal, Surabhi, 'Fresh legislation may replace Data Protection Bill', 17 February 2022, The Economic Times, *available at* Fresh legislation may replace Data Protection Bill - The Economic Times

[117] Malik, Rupinder and Sriram SL, 'Data Protection Bill, 2021: Paradigm shift in compliance', 4 March 2022, The Economic Times, *available at* Data Protection Bill, 2021: Paradigm shift in compliance

[118] Bharti, Aprajita and Iyer, Nikhil, 'Data protection bill: Don't mule the unicorn', 19 May 2022, The Economic Times, *available at* Data protection bill: Don't mule the unicorn - The Economic Times

[119] Rao, Shrinidhi and Grover, Kanupriya, 'How Will the Proposed Data Protection Law Affect Your Startup?', 15 March 2022, Inc 42, *available at* How Will the Proposed Data Protection Law Affect Your Startup?

[120] *Ibid*.

[121] Moorthy, Swathy, 'PDP Bill recommendations will have higher compliance burden on start-ups: IAMAI', 17 December 2021, Money Control, *available at* PDP Bill recommendations will have higher compliance burden on start-ups: IAMAI

[122] Bharti, Aprajita and Iyer, Nikhil, 'Data protection bill: Don't mule the unicorn', 19 May 2022, The Economic Times, *available at* Data protection bill: Don't mule the unicorn - The Economic Times

[123] Gupta, Prince, 'Children's Data Protection', January 2022, CCIER *available at* https://cuts-ccier.org/pdf/bp-childrens-data-protection.pdf

[124] 'Committee's recommendations on Data Protection Bill might lead to higher compliance burden on start-ups: IAMAI, 17 December 2021, Best Media, *available at* Committee's recommendations on Data Protection Bill might lead to higher compliance burden on start-ups: IAMAI

[125] Dadhich, Priyanka, 'India's Personal Data Protection (PDP) Bill: What does it mean for individuals and businesses?', 5 May 2022, Znetlive, *available at* India's Personal Data Protection (PDP) Bill: What does it mean for individuals and businesses?

[126] Bharti, Aprajita and Iyer, Nikhil, 'Data protection bill: Don't mule the unicorn', 19 May 2022, The Economic Times, *available at* Data protection bill: Don't mule the unicorn - The Economic Times

[127] Per Rule 4(2), the agency authorised by the competent authority under sub-rule (1) shall designate one or more nodal officer, not below the rank of the Deputy Secretary to the Government of India, for the purpose of authenticating and sending the requisition conveying the direction issued under rule 3 to the **designated officers of the concerned intermediary or person in-charge of computer resources.**

[128] Jaipuriar, Anish, 'CERT-In | Cyber Security Directions 2022: Aimless and Arbitrary?', 5 May 2022, Mondaq, *available at* https://www.mondaq.com/india/fin-tech/1190190/cert-in-cyber-security-directions-2022-aimless-and-arbitrary?email_access=on

[129] Barik, Soumyarendra, 'Cybersecurity norms may make it 'difficult' to do business in India: 11 industry bodies to CERT-In', 28 May 2022, Indian Express, *available in* Cybersecurity norms may make it 'difficult' to do business in India: 11 industry bodies to CERT-In

[130] Malik, Rupinder and Sriram SL, 'Data Protection Bill, 2021: Paradigm shift in compliance', 4 March 2022, The Economic Times, *available at* Data Protection Bill, 2021: Paradigm shift in compliance

[131] Jion Tu, 'Impact of Regulatory Compliance Costs on Business Performance', 2020, *available at* https://www.ic.gc.ca/eic/site/pbri-iafp.nsf/vwapj/Impact-regulatory-compliance-costs-business-perf-5.pdf/$file/Impact-regulatory-compliance-costs-business-perf-5.pdf

[132] Singh, Ritesh, 'How to help small businesses: Cut heavy costs of regulatory and tax compliance, make credit available', 21 November 2019, Times of India, *available at* How to help small businesses: Cut heavy costs of regulatory and tax compliance, make credit available

[133] https://dpiit.gov.in/sites/default/files/EoDB_Newsletter_March_2021-final-v4-02March2021.pdf

[134] Batchelor, Charles, 'Compliance: Central repository can help rules be noted and followed', 8 November 2011, Financial Times, *available at* Compliance: Central repository can help rules be noted and followed | Financial Times

[135] Through Stakeholder Consultation at Techno Hub, Jaipur

[136] 'Measures to reduce compliance burden have multiplier effect on ease of doing biz: Goyal', 28 September 2021, The Economic Times, *available at* Measures to reduce compliance burden have multiplier effect on ease of doing biz: Goyal - The Economic Times

[137] 'How RegTech can transform your regulatory compliance' Thomsan Reutors, *available at* How RegTech can transform your regulatory compliance | Thomson Reuters

[138] Roy, Subhas, et.al, 'TRANSFORMING COMPLIANCE INTO COMPETITIVE ADVANTAGE', Oliver Wyman, 2018, *available at* RegTech on the Rise

[139] Ibid.

[140] Pahwa Ashish, 'What Is RegTech? – Use Cases, Challenges, & Future', 7 May 2022, Feedough, *available at* What Is Regtech? – Use Cases, Challenges, & Future | Feedough.

[141] https://bfaglobal.com/r2a/

[142] 'Regulatory Impact Assessment', OECD, *available at* Regulatory impact assessment - OECD

[143] 'Reducing Unnecessary Regulatory Costs Responding to the Prime Minister's Challenge', March 2021, *available at* REDUCING UNNECESSARY REGULATORY COSTS

[144] 'Simplicity of systems is key to reducing compliance burden', 23 December 2021, Mint, *available at* 'Simplicity of systems is key to reducing compliance burden'

[145] Kulkarni, Amol, 'Institutionalising Regulatory Impact Assessment in India', February 2018, Cuts Ccier, *available at* Institutionalising Regulatory Impact Assessment in India

[146] UK Department for Business, Energy and Industrial Strategy, Better Regulation Framework: Interim guidance, February 2018, *available at* Institutionalising Regulatory Impact Assessment in India

[147] Kulkarni, Amol, 'Institutionalising Regulatory Impact Assessment in India', February 2018, Cuts Ccier, *available at* Institutionalising Regulatory Impact Assessment in India

[148] Singh, Didar, A, 'Regulatory burden on businesses: Here's what India needs to do to reform the British way', 20 December 2022, Financial Express, *available at* Regulatory burden on businesses: Here's what India needs to do to reform the British way - The Financial Express

7
CHAPTER

Impact of Inadequate Digital Infrastructure on Ease of Doing Digital Business in India

Asheef Iqubbal, Senior Research Associate, CUTS International

Overview

To identify the bottlenecks in Ease of Doing Digital Business (EoDDB), CUTS has been publishing a *Discussion Paper Series* on issues that impact digital businesses in India. The role of digital infrastructure in facilitating a conducive environment for doing digital business is one of them. Economists have repeatedly demonstrated that infrastructure plays a critical role in providing supporting components to businesses as it reduces the cost of production and services and strengthens economic growth.[1]

The role of infrastructure in digital business has a similar impact on facilitating digital businesses. This paper unpacks the digital infrastructural constraints that hinder the digital economy's growth and the digital business ecosystem. In its analysis, the paper goes beyond 'connecting the unconnected' framework, in the spirit that connectivity does not necessarily translate into positionality to use services and business opportunities offered by digital technologies.

Further, the paper breaks the entire gamut of digital infrastructure into two parts – soft and hard digital infrastructures. Throughout this paper, an attempt is made to ascertain the role of digital infrastructure and related challenges in EoDDB that can inform policymakers, business leaders and investors. Towards this end, recommendations on the future strategy are made for facilitating EoDDB to protect and expand the commercial ecosystem.

Digital infrastructure can be divided into soft and hard digital infrastructure. The hard digital infrastructure, such as digital connectivity and data centres provides the necessary foundation for digital businesses to function. On the other hand, soft digital infrastructure, such as cybersecurity and public digital infrastructure – India Stack, National Open Digital Ecosystem, Unified Payments Interface, Open Network for Digital Commerce – facilitates a conducive environment for the ecosystem of digital business. Further, digital literacy, language, culture also are critical factors.

Introduction

India aims to elevate the digital business ecosystem and increase the digital economy by US$1tn by 2025.[2] This vision was fuelled in 2015 when the Digital India programme was launched.[3] The flagship programme is directed to transform India into an empowered digital economy, capturing the potential of technology in the Indian economy. Digital India is an umbrella programme that includes multiple efforts around connectivity, skilling and capacity building, amongst others.[4] For the scope of the paper, only the infrastructural aspects of Digital India will be focussed upon. In this paper, digital infrastructure is the assemblage and interconnectedness of hard and soft infrastructures that facilitate the foundation for digital businesses' operations.

Infrastructural constraints (discussed throughout the paper) have been a bottleneck for digital businesses. Digital infrastructure provides the foundation for the digital business ecosystem and creates necessary grounds for the layers of digital business prospects. It helps in improving coordination and outsourcing of workers, services and optimising targeted

advertising. Soft and hard digital infrastructures have multiple direct and indirect impacts on the digital economy. Indirect impact includes increasing the consumer base and easiness in accessing digital services that contribute to digital businesses' growth.

In this Discussion Paper series that focuses on the EoDDB in India, authors have highlighted the direct impacts relating to different issues of *Criminalising Provisions*[5] and *Regulatory Uncertainty*[6] on digital businesses. However, in the context of this paper, which focuses on the role of digital infrastructure in digital businesses, indirect impacts cannot be excluded as it significantly impacts digital businesses.

An efficient digital infrastructure is critical to support digital businesses, economic growth and improving quality of life as it expands the diversity in choosing goods and services. Lending momentum to the aspiration of Digital India and enhancing the infrastructures for the digital businesses, the Government of India (GoI) allocated around Rs100bn in 2022 for the Digital India programme, up from Rs60mn last year.[7]

Countries around the globe are attempting to leverage the opportunities to gain the economic benefits that digital technologies offer. Still, challenges related to digital infrastructures that support digital business remain one of the significant constraints, particularly in a developing country like India. Understanding and anticipating infrastructural challenges is essential when formulating the policies and legislative framework for digital businesses, as it helps in rapidly building products and services and delivering them at scale.

Implication of Inadequate Hard Infrastructure on EoDDB

A substantial body of empirical evidence now suggests that hard digital infrastructure factors such as increased internet penetration and connectivity are positively associated with EoDDB and growth in Gross Domestic Product (GDP).[8] However, the mission of digitising the Indian society and economy has met with considerable infrastructure challenges such as lack of connectivity and data centres. This also impacts GoI's aim of enabling digital services for commerce, education, healthcare and finance.[9]

These services have unmanageable dependencies upon hard digital infrastructure. India's hard digital infrastructure is not adequate to exploit the maximum potential of the digital ecosystem. This section will unpack the role of the hard digital infrastructures that include connectivity, and data centres in EoDDB.

Lack of Digital Connectivity constraints doing Digital Business

Despite all the promises and magnitude to transform the economy, the digital economy's full potential is yet to be unlocked as more than half of the population in India still lacks access to digital connectivity.[10]

Digital connectivity is at the intersection of the digital business with the physical world which means that it is a critical factor within the ecosystem of digital business. The data of economic contribution around the globe demonstrates that a 10 percent increase in broadband penetration yielded an additional 1.25 percent in GDP growth in developed economies.[11] In comparison, the same increase in middle-income countries yielded only an additional 0.85 percent in GDP growth and much lesser growth in low-income countries.[12]

The relation between penetration of broadband connection and economic growth reflects the importance of connectivity in promoting digital businesses. Smooth connectivity reduces the cost of production, coordination, dissemination and collection of information and services for business players.

The evidence from China suggests that the contribution of digital connectivity and integration to the development of China's digital economy has led to an increment of 163.18 percent in 2019 as compared to 101 percent in 2015.[13] In enhancing the digital economy in China, access to connectivity which includes access to the internet, mobile phones and computers/laptops have been instrumental.[14]

This signifies that the development of digital connectivity has a critical role, which further facilitates ease of doing business for digital players. Having access to digital technologies and devices such as mobile/computer and internet is instrumental and has multiple direct and indirect impacts.

Digital connectivity reduces barriers to entry and opens doors for a new generation of entrepreneurs and innovators as it facilitates knowledge and tools to build business and maximise the growth potential. By bringing market barriers down, digital connectivity can be a great leveller. It can enable the smaller firms to reach out to relevant consumers despite the limited capacities of investing resources to attract new consumers.

India's broadband speed is among the slowest in the world and limited accessibility to the internet remains one of the major constraints of digital business in India.[15] Lack of access to digital connectivity harms the scope for the digital business at multiple layers, such as expanding the access to market, particularly for smaller businesses. Bridging the gaps in accessing digital connectivity for small businesses requires more than just gaining high-speed internet access, smartphones and laptops/computers.

For instance, for business owners in remote locations, new internet-based applications enable them to reach potential new customers, grow their businesses and create new jobs, but that is highly dependent on the access to digital connectivity in the region. Consumers' access to digital technologies can support them in selling goods and services online, marketing and advertising, customer service and support, communications and brand loyalty programmes.

For example, in 2016, to enhance rural mobility a start-up was founded in Bihar's Saharsa district – *AryaGo*.[16] Due to the lack of digital connectivity in rural Bihar, the platform has to rely heavily on interactive voice response by setting up call centres. However, despite the platform investing huge resources in developing digitally-mediated infrastructure, it has not been able to receive bookings through the mobile-based application.[17] The reason is poor internet access in Bihar, which stands at 37 percent.[18]

The offline operation of *AryaGo* makes it difficult to maintain and manage customer relations to enhance users' experience hassle free booking of cabs and rather adds extra financial burden which is hard to sustain in the long run for the platform.[19] The lack of digital connectivity constrains the aggressive promotion of their services through online platforms, as they do not have resources for traditional promotional activities. The case of *AryaGo* reflects larger challenges in starting a digitally-mediated business in India, which is not having access to basic digital infrastructure such as connectivity for a major chunk of the population. Although the rural population makes up a major chunk of India, not having enough online consumers in rural areas discourages budding entrepreneurs from innovating and ideating anything based in rural locations.

In Jammu and Kashmir, start-ups are struggling to overcome internet connectivity challenges. Ubair Shah, the co-founder of *e-fruitmandi*, a start-up that aims to connect small and marginal farmers to the market, said that internet connectivity is one of the biggest challenges in Jammu and Kashmir.[20] Many small and medium businesses do not own mobile phones and live in areas where access to high-speed internet is not available, limiting the platform's growth.

Despite significant improvement in connectivity, India's digital businesses' landscape is still struggling to overcome challenges related to access to digital connectivity.[21] India currently does not have adequate mobile data subscription and broadband connections that has multiple direct and indirect impacts on doing digital business. Examples of Bihar and Jammu and Kashmir reflect the challenges of doing digitally mediated business across the country due to poor digital connectivity, particularly in rural locations as they cannot find enough consumers and unstable internet connectivity increases their operational cost.[22]

Further, limited access to digital technologies such as internet connectivity and smartphone/computers limits the business community's adoption and expansion of innovative technology. For instance, only 53 percent of Micro, Small & Medium Enterprises (MSMEs) have adopted digital technologies in India due to the lack of access to digital connectivity.[23]

The Indian economy heavily relies on MSMEs for employment generation but faces greater challenges of external markets due to limited access to digital infrastructure.[24] The economic opportunities generated by these technologies, such as websites, e-commerce, digital marketing and advertising, and social media for enterprises, have not provided critical indirect and/or direct support in expanding their business, particularly to MSMEs, due to the inaccessibility of digital connectivity such as the internet and mobile/laptop. During COVID-19 induced lockdowns, MSMEs who were in position and/or were integrated into the digital ecosystem could sustain their business. Some of them even increased their sales.[25]

However, businesses operating in locations where access to digital connectivity is limited suffered hugely.[26] Access to digital technologies plays a critical role in determining the future of EoDDB. Without adequate digital connectivity across the country, the digital gap will widen, decreasing digital businesses' penetration and negatively impacting EoDDB.

Accelerating Digital Connectivity

Digital India has attempted to provide new energy to India's ambitious expansion of the digital economy by promising greater connectivity.[27] The mission of digitising socio-economic aspects of the country is an umbrella effort that incorporated and/or rebranded earlier policies and programmes such as National Optical Fibre Network (2011).[28]

However, programmes under Digital India have been poorly implemented, sometimes due to the lack of a backing legislation, but often owing to poor planning and foresight.[29] For instance, National Optical Fibre Network was rebranded in 2014 as BharatNet, to extend the existing optical cable fibre network from the Block Headquarters to 2.5 lakh Gram Panchayats (GP). Phase 1 of the programme missed the deadlines and fell apart.[30] Till June 2021, only 60 percent of GPs had been made service-ready and just 34 percent of these panchayats had been provided with a Fibre to the Home (FTTH) connection.[31]

Access to digital connectivity depends on multiple factors, such as geographical location. Similarly, internet penetration in rural areas is only 29 percent against a national average of 51 percent.[32] There is a persistent income-based digital divide among households as well.[33]

In July 2021, the Union government approved a revised strategy for the BharatNet project, with expenditure leading to Rs40mn.[34] This would be implemented through the Public-Private Partnership (PPP) model in 16 states.[35]

A 2020 report by the Standing Committee on Information Technology remarked on the absence of measures to deliver internet services to end-users and bureaucratic delays in granting tenders.[36] The Comptroller and Auditor General of India on the BharatNet also underlined similar reasons for the poor project implementation.[37]

Excessive downtime of Optical Network Termination that converts fibre signals into digestible information in the form that the devices can understand, hurting the smooth and stable internet connectivity.[38] Fibre networks/connectivity are critical for businesses as they provide symmetrical – upload and download – and stable high-speed connectivity. There are also severe disparities between states, with the Northeast faring the worst, partly because of challenging terrain, rain and floods, all of which should have been part of contingency planning. The terrain and the climate in the region are not classified information.[39]

Further, India has also been left behind in deploying 5G Internet connectivity compared to its global counterparts such as South Korea, China and the United States of America. 5G is expected to cover one-third of the global population by 2025, but India has not even started auctioning 5G spectrum.[40] If India aims to boost the digital economy and EoDDB, it should migrate from 3G and 4G internet connectivity to 5G at the earliest, as slow rollout is a bottleneck in doing digital businesses.

Sectoral regulator Telecom Regulatory Authority of India (TRAI) has been trying to minimise the infrastructural constraints in rolling out 5G. In this regard, TRAI had released a consultation paper stating that street furniture and public structures can be instrumentalised for deploying small cells and aerial fibre.[41] This might help India roll out 5G at scale as it will reduce the capital expenditure. However, an auction of 5G spectrum was expected to be held in 2021, but it has been postponed to 2022. There are multiple reasons for delaying the auction including network providers asking for more time to test the technology. At the same time,[42] some reports claim that the government needs to do a lot of work on making the necessary spectrum available.[43] The cold response in rolling out 5G networks will hurt the economy and digital business, allowing faster and smooth connectivity for everyone.

In an attempt to bridge the gaps in accessing the internet, Prime Minister Wi-Fi Access Network Interface (PM-WANI) was initiated by the Indian government in 2021. The scheme aims to deploy large-scale public Wi-Fi hotspots and access points at the local stores and neighbourhood shops as availed

by the Public Data Offices (PDO) without any licence, fee or registration. PDOs will be set up on similar lines as the old-school Public Call Offices (PCOs).[44]

PM-WANI aims to be a low-cost internet option for the underserved populations of the country, subsequently enhancing the ecosystem of the digital business across the length and breadth of the country. Still, its success in providing meaningful connectivity remains to be seen. Enhancing connectivity through PM-WANI might not directly facilitate doing digital business, but it will certainly have multiple indirect impacts. Increasing the connectivity will expand the consumers' base and help onboard small and medium enterprises into the digital business ecosystem such as e-commerce.

However, public WI-FI networks have not been unfamiliar to the data breach and privacy related concerns. Accessing any website that is not HTTPS certified through public WI-FI can increase vulnerability related to data security.[45] The governing framework of PM-WANI falls short in specifying robust information security mechanisms in order to ensure secure connections.[46] For instance, any actor can become a PDO as it has removed the registration process to become a PDO but there are limited checks and balances in terms of security and privacy.[47] Further, as there are no registration, verification and authentication requirements for a PDO, any PDO can be a rogue network more susceptible for hacking and attack on personal and non-personal data of the users.[48] Anyone can access the internet services under PM-WANI by just completing KYC process which is not an adequate security mechanism either,[49] thereby it creates an opportunity for the hacker to get unfettered access to unsecured devices of legitimate users on the same PDO network. As India is yet to mandate data protection legislation, it poses risks for both users' data and any personal or sensitive information entered for the purpose of authentication.[50] There should be a periodic audit mechanism to keep a check on the rouge networks acting as PDO, it will enhance the security and trust of the user within the PM-WANI scheme.

Furthermore, PM-WANI mandates that users' data must be stored for a year for compliance and legal provisions, the rule states, "PDOA shall make necessary provisions for storage of user data for one year to ensure compliance with legal provisions, as required."[51] The framework further states "subject to terms and conditions of the Registration, the App Provider, PDOA and Central Registry Provider will take all necessary steps to safeguard the privacy and confidentiality of any information about a third party to whom it provides the service."[52]

However, aforementioned rules do not clearly spell out the data security measures and how the collected data will be managed. The storage of the users' data raises concerns of privacy and surveillance despite the government stating that all stored data under PM-WANI will be safe and secure. The PM-WANI framework does not define whether this data will be accessed or not by the government and its agencies.[53] If accessed, then the grounds of such access are not provided and in the absence of a data protection law and surveillance framework there are no checks on the powers of the government and its agencies.[54] Any executive orders or legislation which accesses user's data, infringe upon the right to privacy, should be required to adhere to the principles of legality, necessity, and proportionality established in the *K.S. Puttaswamy judgement*.[55] In light of the above and in absence of a robust data protection mandate and adequate surveillance framework, the concerns of data security around the PM-WANI scheme will remain unaddressed.

Along with the GoI, multiple state governments are also navigating ways to provide internet connectivity to foster digital businesses. For example, in Rajasthan, the L-route server has been operationalised at Bhamashah State Data Centre to provide smooth digital connectivity to facilitate digital businesses.[56] The server has been established in association with the Internet Corporation for Assigned Names and Numbers (ICANN).[57] The server is independent of any Domain Name System (DNS), which means that internet services in the state will not be interrupted even in the case of natural calamities.[58] Further, the Uttar Pradesh government has promised free Wi-Fi in villages to enhance connectivity and integrate the society into the digital ecosystem under the '*smart village*' mission.[59]

Kerala was among the first states to declare internet as citizen's basic right.[60] The Kerala government has recently promised to provide free internet connectivity to the people living at the socio-economic margin under the Kerala Optical Fibre Network (K-OFN) project.[61] Other states are following similar models to provide stable and faster digital connectivity that will be critical in expanding the scope of digital businesses in remote and semi-urban locations.[62]

The Supreme Court of India, in Anuradha Bhasin & Ors v. Union of India has stated that the right to carry on any trade or business using the internet is protected under the Indian constitution.[63] The Kerala High Court also delivered a verdict by arguing that access to the internet is a basic right and cannot be denied on social and moral policing.[64]

Internet Shutdown – Disrupting Digital Business

However, despite the Supreme Court's order, internet shutdowns have become a pathological response to maintaining law and order situations in India by central and state governments.[65] Internet shutdowns crush businesses and enterprises that heavily rely on digital connectivity to function. The Indian Council for Research on International Economic Relations (ICRIER) published a report in 2018 noting that India lost more than Rs220.3bn due to internet shutdowns during 2012-2017.[66] According to the UK-based privacy and security research firm, Top10VPN, India suffered the biggest economic loss in the world in 2020 due to internet shutdowns, adding up to 8,927 hours and US$2.8bn losses.[67]

Internet shutdowns hurt small entrepreneurs more severely and to the extent that they have to close down their business operations and find a job to survive. Alam Gul, an entrepreneur from Jammu and Kashmir, started a software firm by investing his savings in 2018.[68] In 2019, the GoI shutdown the internet in Jammu and Kashmir for the longest time in any democratic country. Gul's venture was unable to function due to the unavailability of the internet, subsequently failing to deliver the services promised to the clients.[69] Internet shutdown broke his spirit and now he is wary of starting another venture.[70] Entrepreneurs cannot find any investors as they fear that internet services will continue to be disrupted in Jammu and Kashmir.[71]

According to the *Kashmir Chamber of Commerce and Industry (KCCI)* estimates, Kashmir's economy alone suffered a loss of Rs 17,000cr (1,70,000 million) due to the communication lockdown in the wake of the abrogation of Article 370.[72] *The Cellular Operators Association of India (COAI)* has evaluated an estimated Rs 2.4 crores (24 million) per hour of revenue loss to members during internet shutdowns.[73]

Fast Beetle, an online logistic venture, was nascent when the internet service was suspended in Jammu and Kashmir. Until August 2019, *Fast Beetle* delivered 15000 orders across Jammu and Kashmir and regularly provided employment to 11 people. However, the shutdown broke down the whole business chain of Fast Beetle, forcing it to shut its operation for almost eight months.[74] Its co-founder said that disruption of internet shakes stakeholders' confidence, including investors. Despite liking the e-business model, investors are not willing to invest in a start-up based in a region where connectivity is not stable.[75]

Negative impacts on digital businesses, livelihood and innovations are evident as India continues to top the chart in shutting down the internet globally.[76] It has been challenged in court multiple times. The due process of shutting down the internet was laid down in *Anuradha Bhasin v. Union of India,* challenging the prolonged internet blockade in Jammu and Kashmir.[77]

The Supreme Court stated that it was illegal to shut down the internet indefinitely under Indian law. The court further stated that the order for internet shutdown must satisfy the requirements of necessity and proportionality.[78] Further, it placed requirements on the government to make internet shutdown orders public and subject to judicial review.[79] The court also mandated that such shutdowns need to be temporary and reviewed regularly.[80] The frequent and protracted shutdown of the internet has long been in contest with international and constitutionally guaranteed civil, political, social, and economic rights. Its implication on EoDDB is deep as it shakes the business community's confidence.

However, despite Supreme Court's ruling, India continues to shut down the internet. Recently, Rajasthan government shutdown internet in Jhunjhunu in view of Holi Procession in March 2022.[81] Similarly, West Bengal Government also shut down the internet in several districts of the state to prevent cheating in exams in March 2022.[82] The High Court in West Bengal stayed the government's order of suspension because it did not disclose the necessity for the shutdown.[83]

More recently, in Jodhpur, a district in Rajasthan, internet was suspended for an undetermined period, violating the Supreme Court's order in which it said internet services could not be suspended for an undefined period.[84]

Suspension of internet and EoDDB do not go together. If India aims to boost the digital economy and provide a conducive business environment, it needs to recalibrate the frequent suspension of the internet that is being frequently done on the grounds of public order and national security.

On shutting down the internet, the government's position of national security and public order continues to dominate the discourse. However, the losses in EoDDB include missed opportunities, jobs, livelihoods, access to health and education, and government services which need to be considered.[85]

Development of Data Centres

Digital businesses need to store data to enhance services, consumers' experience and minimise the cost of production. This requires data centres to host, process, analyse and access their data directly or indirectly. Digitally-enabled business enterprises, such as cloud service providers, fintech, health tech, and edtech would require comprehensive backend digital infrastructure in the form of data centres to cover users' demands. The convergence technologies and other factors offer a new set of economic avenues such as data centres. Quality, availability and accessibility of data centres are critical in promoting the digital business ecosystem.

Demand for data centres would grow exponentially in India due to the growing use of Information and Communication Technology (ICT)-enabled services. Particularly, the need for data centres is paramount in the context of the proposed data localisation mandates and Reserve Bank of India's (RBI) rules[86] that require data storage within national boundaries. Meeting the demand for data centres will be critical in facilitating the digital business ecosystem, but there are infrastructural challenges in setting up the data centres in India. There are 749 million active internet users in India[87], but the country has an abnormally low, 80 data centres[88], compared to Europe's 1978 data centres[89] for 372.43 million internet users.[90]

Further, the traditional data centres cannot support the increasing complexities of digital business such as cloud computing and social media.[91] Digital businesses require hyper-scale data centres that would ensure better access and analysis of large volumes of data which will add value to their supply chain and enhance customer experience by more significant levels of personalisation.[92]

In this context, it is important to talk about the challenges such as the absence of legislative backing in establishing data centres, uncertainty around data storage, clearly spelled out standards and hard infrastructures that include power supply, land for setting-up data centres in India, which might have a negative impact on doing digital businesses in India.

Riding on the increasing penetration of ICT-enabled services such as smartphones, social media, e-commerce and entertainment platforms, India aims to take advantage of data centres services due to the country's exponential growth of data creation and consumption. The Finance Minister, Nirmala Sitharaman, in her 2022 budget, extended the infrastructure status to data centres to avail credit and manage resources.[94]

Constraints present here challenge setting up data centres. For instance, land and power, high speed and stable internet connectivity are necessary to establish the data centres, and such infrastructural requirements are not present in smaller cities. The average power supply required is between 15-100 MW and 3-12 acre land with high bandwidth to develop the data centres.[93] These requirements also mean that developing data centres is a high capital investment task and needs governments' support to facilitate infrastructure and investment.

India's Data Centre Policy, 2020 states, "drive necessary regulatory, structural and procedural interventions for enabling ease of doing business in the sector, attracting investments and accelerating the existing pace of Data Centre growth in the country."[95] Different state governments also propose their own data centre policies to attract investment. For instance, the Telangana government in 2016 published a document that aimed to attract investments in data centres, and the Tamil Nadu government also published a similar data centre policy.[96]

Along with the infrastructural challenges, Data Centre Policy, 2020 aims to simplify the complex clearance policy for setting up data centres in India, but no clear mechanism has been laid down in the draft.[97] The draft policy states that Data Centre Economic Zones (DCEZ) will be set up to promote data centres in India. However, India's experience rolling out similar schemes has not brought intended success. For instance, Special Economic Zones (SEZ)[98] and Mega Food Park[99] suffer from multiple challenges such as unpredictable taxation and limited incentives to expand, need to be taken into account.

In addition to these, Data Centre Policy 2020 does not talk about issues related to cybersecurity which are essential to ensuring sustainable growth of data centres in India. Cyberthreats will continue to hunt business, consumers, and government without establishing safe and secure data centres, and India has already been performing poorly in risks related to cyber security. Building desired data centres for business and end consumers will be critical to ensuring a safe, transparent, and sustainable ecosystem for digital business.

Implication of Soft Digital Infrastructure on EoDDB

Access to hard digital infrastructure – uninterrupted and faster internet connectivity, smartphone, laptop/computer and data centres – cannot be seen in isolation from soft digital infrastructures that comprise digital literacy, culture and language. Empowering the underserved population and facilitating digital business involves the availability of digital connectivity and affordability, positionality that can allow them access to a wide range of potential that technological development offers.

Access to the hard digital infrastructure requires understanding what digitalisation means in its widest possible sense and imagining alternatives to the traditional digital business approach and participation in commercial activities. This section will unfold the issues related to digital literacy, language and cultural barriers in EoDDB.

The section will also unpack India's public digital infrastructure, including India Stack, Digital Payment Infrastructure, Open Network for Digital Commerce, and National Open Digital Ecosystem. Public digital infrastructure is an attempt to democratise the access of technology that can be reprogrammed for small businesses, start-ups and budding entrepreneurs to utilise.[100]

A digital ID card has lowered the cost of confirming an individual's identity, and open access software standards facilitate digital payments between banks, fintech firms and digital wallets. All these initiatives have provided better mechanisms for doing digital businesses in India. However, there are multiple challenges related to open digital technologies. Along with these, issues related to cybersecurity will be discussed as safe and secure cyberspace has a positive association with EoDDB.

Digital Literacy, Language and Culture

Digital literacy is defined as the ability of individuals and communities to understand and use digital technologies for meaningful actions within life situations, including operating a computer, laptop, tablet and smartphone.[101] If at least one person within a household can operate the devices, the household is considered digitally literate.[102] Only 38 percent of the households in India are digitally literate, whereas about 61 percent of households in urban and only 25 percent of households in rural are digitally literate.

Online commercial activities in India have gained significant momentum in the recent past, but consumers have not put total confidence in the digital ecosystem.[103] Along with meaningful access to digital infrastructure, digital literacy is critical in establishing confidence among stakeholders.

The lack of digital literacy in Indian households is a barrier for digital businesses to penetrate rural and urban households.[104] This highlights that, digital businesses are yet to fully realise the market potential of increasing digital adoption in India. In EoDDB terms, access to digital connectivity brings together businesses and consumers through digital connectivity and applications but it cannot be separated from their required skill and knowledge.

The GoI initiated the National Digital Literacy Mission (NDLM), Digital Saksharta Abhiyan and Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) with the vision to empower at least one person per household with digital literacy skills by 2020 to integrate the people in the digital ecosystem.

Subsequently improving EoDDB. NDLM is an attempt to complement the Digital India mission to transform each household into digitally literate.

However, the programme fell short on multiple fronts due to lacking funds, resulting in poor implementation and execution.[105] INR 2,350 crore was required for 2017-19, only INR 536 crore has been allotted to the scheme.[106] Additionally, GoI used a method that was expensive and flawed, training people through computers that require high investment infrastructure and broadband internet connectivity, while largely Indian people have been using internet through smartphones.[107]

Overcoming these inequalities is critical for EoDDB and requires an equal emphasis on digital infrastructures and skills development. Limited digital literacy in rural areas impacts the EoDDB, as MSMEs find it challenging to attract skilful individuals who can instrumentalise the digital ecosystem to drive economic growth. A large pool of skilful and digitally literate individuals is concentrated in urban pockets due to better educational opportunities and thus have higher chances of getting employment. These factors also negatively impact the ecosystem of digital business in rural areas.

Like digital literacy, cultural and linguistic barriers also affect the ability of the people to access and avail products of digital businesses. Limited access to different regional languages and dialects on the internet hinders digital business growth as consumers are wary in case of a dispute. Online commercial platforms provide the redressal mechanism. The process such as bots and emails are often not easy to navigate.

For instance, most businesses and consumers prefer to operate and interact with their consumers in their regional languages. A Common-Sense Advisory Survey with 8709 online consumers in the Business to Consumers (B2C) segment in 29 countries reported that 75 percent of respondents preferred to do online transactions if the information was in their native language.[108] About 60 percent confirmed that they rarely or never bought from an English-only website because they cannot read.[109] The 956 business-to-business (B2B) survey shows a similar sentiment toward doing business in their native language.[110]

Whether B2B or B2C, consumers prefer to do online transactions in their native language.[111] This reflects the importance of language in enabling digital commercial activities. In India, leading e-commerce companies like Amazon and Flipkart have invested and expanded the subsequent 100 million users by providing text and voice-based consumer support in regional languages.[112]

However, it would be difficult for smaller businesses to provide multilingual content due to limited resources and capacities. Compared to conventional offline consumers, increasing digital technologies and associated risks related to quality and online financial fraud have also emerged. Generating awareness is critical to harnessing maximum potential digital business. EoDDB demands more digital interactions between consumer and business platforms and creating the infrastructure and an environment – literacy, culture and trust – that is conducive to commercial activities is critical.

Increasing Cases of Cybercrime

With increasing adoption of digital technologies but associated lack of understanding about the importance of cyber security, businesses and consumers are increasingly falling prey to cybercrimes. Cybercrimes are an emerging and increasing concern for businesses and people vis-a-vis disruption of services, privacy and security concerns, including data breaches, ransom attacks, and loss of commercial reputation, negatively impacting the digital business ecosystem.

Cyber-attacks in India were reported to have increased by about 300 percent in 2020 compared to the previous year, which had cost Small and Medium Businesses (SMB) in India more than Rs 3.5 crore.[113] According to a survey, 52 percent of people do not know how to protect themselves from cybercrime, and even more, 68 percent say it is difficult for them to determine the credibility of their information. In a period of just 12 months, over 27 million Indian adults experienced identity theft. More importantly, three out of four MSMEs in India witnessed a cyber-attack in 2020. It is critical to note that the cost of a cyberattack is not just material.[114] The loss is colossal in reputation, loss of consumers and damage to profit margins. Globally, the cost of cybercrimes is high and rising as well.[115]

MSMEs are more prone to cybercrimes due to a lack of awareness and/or knowledge, lack of skilled personnel, and limited capacity to invest resources in building capabilities that will protect them. For instance, MSMEs do not always know if they have been attacked or breached.[118]

Since India is the second-largest online market globally with over 749 million internet users and aims to instrumentalise the user's database to boost the digital economy by enhancing EoDDB, safe cyberspace will be critical for the intended aim.[116] Cybercrimes in India have implications for commercial activities across the globe because of the sheer size and volume. Many data files and online activity important to the world are being generated and consumed in India, so the rising crimes here and its ability to tackle growing cybercrimes concern EoDDB.[117]

Similarly, business owners may not know how much and what type of data has been leaked.[119] Additionally, MSMEs may also hesitate to report cyberattacks to law enforcement agencies as these businesses fear a loss of reputation by exposing their vulnerabilities.[120]

Minister of State for Electronics and Information and Technology (IT) Rajeev Chandrasekhar said, "the government is committed to ensuring that the internet in India is open, safe, trusted and accountable for all users".[121]

Currently, the response to cyber security threats can be taken under the Information Technology Act, such as hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft, and the Indian Penal Code punishes criminal offences in cyberspace defamation, cheating, criminal intimation and obscenity.[122]

In accordance with IT laws, the Indian Computer Emergency Response Team (CERT-In) was created in 2004 to take care of incident response, and the National Critical Information Infrastructure Protection Centre (NCIIPC) was created in 2008 to look after critical infrastructure from the threat of cybersecurity.[123] Recently, GoI mandated that Indian companies report any cybercrime within six hours under CERT-in.[124]

Additionally, The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties Rules 2013 (CERT Rules) has been established as the nodal agency responsible for collecting, analysing, and disseminating information on cyber incidents and taking emergency measures to contain such incidents. India also enforces Companies Management and Administration Rules 2014 (CAM Rules) framed under the Companies Act 2013, which mandates companies to ensure that electronic records and security systems are secure from unauthorised access and tampering.

CERT-in demands real-time data from service providers such as intermediaries and data centres in India. However, there are multiple layers in cyber fraud and/or cybercrimes and disclosing information within six hours and without any oversight, access to the data in nearly real-time might be tricky and raises the question of surveillance.[125] These mandates will negatively impact EoDDB, as NordVPN, a leading VPN provider, may pull out of India due to proposed changes in CERT-in, which mandates storing users' data for five years.[126]

Along with flawed implementation, these mechanisms cannot adequately address the dynamic nature of cybercrime due to the lack of coordinated approach.[127] There is no uniform cybersecurity architecture that unifies the efforts of all these agencies to be able to assess the nature of the threat and tackle them effectively.[128] Lack of inter-agency coordination and unclear demarcation of roles and responsibilities weaken the efficiency and effectiveness of cybersecurity.[129] To this end, the government is expected to introduce a national cyber security strategy to provide guidelines and build capacities in tackling emerging cyber threats. Still, the process needs to be accelerated as effective cybersecurity mechanisms positively impact the digital business environment.[130]

Public Digital Infrastructure – India Stack

India Stack is a project of creating a unified software platform that will facilitate India's digital business ecosystem. "India Stack is a set of Application Programming Interfaces (APIs) that allows governments, businesses, start-ups and developers to utilise a unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery".[131]

The stack consists of four layers of infrastructure and standards: (i) digital identity, which features the Aadhaar digital ID system that allows for identity verification and the mapping of information across

datasets; (ii) an interoperable payments interface which is Unified Payment Interface (UPI); (iii) digitalisation of documentation and verification which can be instrumental in the verification of digital documents that can replace traditional paper analogs; and (iv) a consent layer that will involve the operation of data fiduciaries that act as intermediaries between individuals and financial companies.[132]

Pillars of India Stack have been introduced gradually in the last decade in India, except for the consent layer. The first two, Aadhaar and UPI will be discussed in the next section of this paper. In this section, the consent layer is discussed.

Consent layers have not been fully developed and operationalised in India but probably it would be based on MIT Media Lab's Open Personal Data Store (OpenPDS) system, allowing users to collect, store, and give fine-grained access to their data while protecting their privacy.[133] It enables the user to view and reason about the data collected. The user would own secured space, PDS acting as a centralised location where their data resides.[134]

The user can then control the data flow and manage fine-grained authorisations for accessing his data. The individual data ownership model would fundamentally impact the digital business ecosystem from a business standpoint. The business would have to largely reprogram its digital architecture based on the individual's data.

Digital business would be dictated by the users' justification of services and data, and services can be rated and evaluated, accordingly. Interestingly, India Stack can revoke the access of the data from any business platforms if the concerned person expresses their withdrawal.

Currently, data is being collected and stored by hundreds of different goods and service providers. Data, particularly, metadata is yet to realise its full potential due to fragmentation that makes the data inaccessible to innovative services and often even to the individual who generated it in the first place. Additionally, the lack of access and control over the data is fuelling growing concerns about associated risks. The data ownership model enabled by OpenPDS can potentially foster alternatives to the current data-selling and advertising-based business model.

India Stack potentially aims to unlock the economic values of the data that includes digital business opportunities to provide hardware for data collection, storage for metadata, or algorithms for better-using metadata by keeping software for data collection and data management open-source.

Subsequently, removing the barriers to entry for new businesses allows the most innovative algorithmic companies to provide better data-powered services. This will facilitate EoDDB for new entrants.

However, the technologies used in the OpenPDS are complex and would not be easily available in India.[135] Moreover, there is still a lack of clarity on how this would be operationalised, limiting the understanding around it.

Online Payment Infrastructure

New-age digital payment modes, such as UPI, Aadhaar-Enabled Payment System (AePS) and Bharat Bill Payment System (BBPS) are crucial to India's cashless economy.[136] Riding on Open Banking such as UPI, launched by the National Payment Corporation of India (NCPI), digital payment infrastructure has seen an exponential boom in India.[137]

This has allowed fintech platforms to innovate and create a strong foundation for digitalisation and cross-selling other financial products and services such as GooglePay, ÿþPhonePe and ÿþBharatPeÿþ. Interoperability enabled by public sector API has been critical in the wide acceptance of application-based online financial transactions as well as it has generated competition among the fintech players.[138]

Cheap internet data, increasing penetration of smartphones and India's biometric identity card provided the fertile ground for digital payment in India.[139] India's biometric identity Aadhaar – built on a unique 12-digit identification number for each Indian resident – has become a critical component in boosting digital payments.[140]

Aadhaar has been India's most ambitious public digital infrastructure project to provide a single identity card to Indian people. It allows seamless integration of cash transfer between consumer-to-

consumer and consumer-to-merchant through mobile applications. It does so by bringing e-KYC (Know Your Customer), turning an Aadhaar number into financial address, e-signature and UPI.[141]

Determining the root cause behind any dispute is time-consuming and complex. Online financial transactions involve multiple players: a bank that accepts the transaction; a network such as Visa, Master, Rupay; and the bank where consumers hold their account. These complexities have been a bottleneck in facilitating digital business, leading to a pile-up of credit reversal failures.[145]

While using UPI does not require an Aadhaar ID, Aadhaar has facilitated e-KYC compliance for opening bank accounts needed to access the UPI system.[142] Further, Aadhaar has enabled the digital ecosystem involving several APIs.

These APIs allow public and private service providers to authenticate identity using the data biometrics, demographics, and links to individual phones registered with Aadhaar to facilitate authentication using a One Time Password (OTP).

The Reserve Bank of India (RBI) has also started Payments Infrastructure Development Fund (PIDF). The fund will be spent to subsidise deployment of Points of Sale (PoS) infrastructure (both physical and digital modes) in tier-3 to tier-6 centres and north-eastern states.[143]

In 2020, India was among the top countries globally, with 25.5 billion online financial transactions.[144] Although there are challenges relating to dispute resolution that fintech platforms are facing, it demands attention to enhance EoDDB. Most fintech players approach dispute management through phone calls or digital channels like WhatsApp and Email.

Other concerns related to privacy and security continue to be a challenge for fintech platforms.[146] In digital payments architecture, vulnerabilities related to privacy are at many layers, including poor technical mechanisms and unethical data collection practices. For example, the front end is a biometric capture device in a digitally enabled payment system. The backend comprises consumer Aadhaar data linked to the bank account and in between these two, data transmission systems function.[147] The authentication is done through passwords. However, data breaches in the digital payment ecosystem, unethical data collection have not been uncommon. One of the major fintech platforms has repeatedly faced massive data breaches that diminish users' confidence in the digital payment ecosystem.[148]

The absence of data protection mandates also reduces confidence in the digital ecosystem. In addition to this, digital payment also excludes people living at the socio-economic margins. The success of a cashless economy will heavily rely on how much it will enhance inclusiveness and secureness in online financial transactions. This will lead to a better ecosystem for doing digital payment business in the country.

National Open Digital Ecosystem

India is deliberating the implementation of another open public digital infrastructure – the National Open Digital Ecosystem (NODE). The Ministry of Electronics and Information and Technology released a white paper in 2020 and laid down the broader principle of the NODE.[149]

The white paper states that NODE will consist of a three-layer mechanism: a delivery platform which is the technological aspect; a governance framework that will anchor the technological component; and a community that will develop and new on top of it to deliver shared values. The open digital ecosystem aims to encourage competition by breaking the entry barriers and spur innovation and investments, thus facilitating a business-friendly digital environment.

Delivery platforms, consisting of entrepreneurs, business and public agencies, will facilitate the delivery of services and solutions to the end-users. This will be modular/reusable, scalable and interoperable to unlock maximum benefits. Moreover, it can be flexibly integrated with other applications through open APIs, e.g. Aadhaar authentication, e-KYC. Personal and community information/ records, will be provided by 'single source of truth' e.g. financial data, identification data, civil registries, land registries, and Exchanges which facilitate flow of data being generated by governments, businesses and individuals, e.g. Indian Urban Data Exchange (IUDX), Account Aggregators.

The governing framework for NODE would consist of multiple stakeholders such as institutions that own the delivery platform, builders who develop solutions on it, and end-users who consume services and/or participate in designing solutions. Since openness in data sharing increases the vulnerabilities of the associated risk of misuse and manipulation of the data, NODE would have a strong governance mechanism to ensure fair value sharing while keeping stakeholder behaviours in check, with both preventive and corrective measures.[150] A vibrant community of partners will drive NODE to unlock its values. The community consists of government, foundations, think tanks, businesses and entrepreneurs who will transact and collaborate via the NODE to create new user-centric solutions.[151]

NODE will enable business communities and entrepreneurs to innovate and ideate new technology-centric solutions, subsequently providing an alternative vision of digital ecosystems to the dominant big tech-controlled digital ecosystems. It will be critical in supporting budding entrepreneurs and smaller businesses as they can ideate and build innovative ways of doing digital businesses. However, this is just one of the potentials of the NODE, but to achieve the stated objective, it needs careful implementation.[152]

NODE, an open digital ecosystem, will potentially break the wall of the current platform-centric model where everyone has to use the same platform/application to enable transactions between them — subsequently promoting interoperability and EoDDB, particularly for smaller players.[153]

India has experience developing an open digital ecosystem and it must use its experience to enhance the inclusivity of small businesses, start-ups and budding entrepreneurs. If it is not designed and incorporated while developing the NODE, it might lead to monopolisation and concentration of resources among a few hands. The top-down approach in developing these ecosystems that aim to democratise public digital infrastructure access might be counterproductive.[154]

There is a lesson to learn from past experience. For instance, under the 'Bulk Data Sharing Policy' the GoI intended to monetise the database of vehicle registration certificates, citing benefits to the 'transport and automobile industry'. The government reserved Rs 3 crore for accessing the data, which would have become an entry barrier for small businesses.[155] In the context of NODE, the government needs to be careful about entry points that are critical in fostering innovation and fairer digital business.

The white paper also raises some concerns about objective and scope of NODE, including integration with existing architecture, policies and regulations. The scope is broad as it assumes, throughout the paper, that operationalisation of NODE will improve the overall functioning of the sector. The broader objective and scope of the NODE also raise concerns about the harm such as functioning creep, surveillance and other data-related risks as the white paper does not clearly spell out the stakeholders within the NODE.

There is almost no clarity on who can access the NODE and its purpose. In addition to this, the white paper paid limited attention to harmonisation of existing public digital infrastructure, policies and regulations. It mentions initiatives such as National Digital Health Blueprint (NDHB), National Urban Information System (NUIS), Digital Infrastructure for Knowledge Sharing (DIKSHA), and India Enterprise Architecture (IndEA). However, how these initiatives that require different ministerial coordination, will be integrated or built off these initiatives when implemented remains to be seen. If they are not seamlessly integrated might create friction, negatively affecting the EoDDB.

Open Network for Digital Commerce

The Department for Promotion of Industry and Internal Trade (DPIIT) went live with its Open Network for Digital Commerce (ONDC) project on a limited scale.[156] The ONDC aims to democratise the digital commerce ecosystem by shifting from platform-centric models to an open network.[157] This would enable small businesses to access processes and technologies largely deployed by large e-commerce platforms such as Amazon and Flipkart.

Operationalisation of ONDC that includes onboarding of sellers, vendor discovery, price discovery and product cataloguing could be made open source on the lines of the UPI. ONDC will work on two ends — the seller and the buyer sides.[158]

On the seller side, players such as *GoFrugal*, an enterprise resource planning company, and *Digiit*, a digital business platform, are engaged. While on the buyer side, the interface is being built on *Paytm* and will be expanded when the ONDC is rolled out to its full potential.[159]

Lack of interoperability brings multiple problems for digital business, such as portability of trust. E-commerce allows businesses as well as consumers to build a reputation through the transaction enabled by the platforms, which has a critical value in doing business in recent times. However, if a business is keen to port to another platform in a platform-centric model, they lose all the hard-earned reputation and trust. They have to start the business from scratch again even though the data and reputation belong to them. The lack of portability among e-commerce platforms disincentives the business as they can neither transpose nor migrate. The loss is significant mainly for smaller businesses as they have limited capacity to repeatedly build their reputation.

ONDC will help enhance the visibility of the service delivery platforms and/or sellers that help MSMEs reach out to a greater consumer base with limited resources. This will be done through operational mechanisms of ONDC that will facilitate interoperability and buyers and sellers can transact no matter what platform/application they use. ONDC is intended to ensure that sellers and buyers do not need to be on the same platform, as has been done in the fintech ecosystem.

Additionally, if anyone hopes to do business on multiple platforms, they must maintain separate processes, which adds the financial burden on the platform as each e-commerce platform has its terms and conditions. This constrains participation in the digital business ecosystem. The ONDC intends to go beyond the B2C and cover any digital commerce domains, including wholesale, mobility, food delivery, logistics, travel and urban services. The open network, ONDC is being developed, will have multiple effects on businesses, consumers, application developers, governments, and other relevant participants by enabling an interoperable and open playground for various sections to function and compete.

ONDC aims to unlock innovation and scale within digital commerce by democratising the ecosystem. Unlocking will also open up new digital business opportunities for budding entrepreneurs to ideate and innovate in multiple areas such as logistics and warehousing and provide specialised services to buyers and sellers as ONDC will be accessible in multiple languages and dialects. However, like UPI, ONDC has some challenges, such as financial fraud, security risk, and duplication of products. The strategic paper on ONDC does not have enough privacy and security safeguards information which demands attention.[160]

Recommendations

Access to Meaningful Connectivity

Digital divide in India is stark and demands urgent attention. From a digital business standpoint, stable and faster connectivity is critical as it has layers of direct and indirect impacts, as demonstrated above. Empowering the underserved population involves the availability of internet connectivity, affordability and positionality that can allow them access to a wide range of potential digital business opportunities. To this end, India needs to close two gaps in accessing the digital connectivity: firstly, those living in dark telecom settings and cannot access the internet; and secondly, those who have access to the internet but their socio-economic situation deprives them of this access.

The policymakers need to focus on specific assessment standards for different user groups, based on which assessment can be made of the type of digital skills required for them. It will help in creating tailored mechanism programmes accordingly. India needs to reprogram its approach to fill the gaps in accessing digital connectivity, such as redesigning broadband policy where particular attention on geographical locations is given, crafting effective public-private partnerships, and promoting infrastructure sharing models that will lessen the financial burden of internet operators, subsequently increasing the integration of digital businesses.

Recalibrate Internet Shutdown

India needs to learn from developed nations on how they are minimising the internet shutdown to avoid disruption in doing digital businesses.[161] Canada declared access to the internet as an essential component in participating in economic activities and quality of life.[162] The German court ruled that the internet is an essential part of life and customers have the right to compensation if the service is interrupted.[163] Finland declared access to the internet a legal right.[164]

If India aims to enhance the digital business ecosystem, access to the uninterrupted access to internet needs to be seen in a framework of essentiality. Evidence suggests that cost of internet shutdowns is too high, particularly for digitally mediated businesses. As the Supreme Court stated, India must recalibrate based on proportionality and necessity. Internet shutdown for an indefinite time hurts the prospects of digital businesses. Internet shutdown mechanisms need to be carefully deliberated and recalibrated to foster confidence among digital businesses, consumers and investors.

Enhancing Cybersecurity

Rise in the adoption of technology has opened a fault line in terms of cyber threat, crime and fraud. The breach in cybersecurity has seen an alarming rise in recent times in India and the cost is not just material, but it impacts the overall ecosystem of digital business activities. If India wants to attract investors and entrepreneurs and sustain the exponential growth of the digital economy, it must strengthen its cybersecurity.

Currently, India's approach is disparate and different actors are working in different directions that need an overhaul where coordinated and robust effort is made to strategise and tackle the cyberthreat. In addition to this, investment in developing safe and secure data storage and skilful individuals who can maintain the security of such ecosystems. Policymakers and the industry should engage more deeply with international cyber security practices, collaborate on improving cybersecurity mechanisms with like-minded countries and actively work on building more robust cybersecurity mechanisms for the country. Providing a digitally safe and secure environment is necessary for digital businesses to function effectively.

Public Digital Infrastructure

Open-source approaches to technologies in India have leaped and it can be instrumental in efficiently developing tailored solutions and opportunities for digital business. In developing open-source digital ecosystems such as UPI, ONDC, NODE, the process should be more participatory and include different stakeholders such as small and medium businesses, budding entrepreneurs, and civil society organisations to minimise unintended consequences such as exclusion, digital monopolisation and risk related to data. Transparent and consultative processes will help inequitable access to the public digital infrastructure with built-in philosophy to reduce entry barriers and frictions.

Public digital infrastructure can be designed to be interoperable and modular structures, on top of which reprogrammed interfaces and databases can operate using APIs. Anyone can reprogram these architectures according to their needs, which can only be done through participatory and consultative processes. The open digital infrastructure that envisions democratising the access of public digital infrastructure must avoid centralisation, which can lead to monopolisation of powers with limited accountability, which is critical for enabling innovation, competition, partnership and user-friendliness.

Endnotes

1 Assessing the Impact of Infrastructure on Economic Growth and Global Competitiveness. *Available at* https://www.sciencedirect.com/science/article/pii/S2212567115003226

2 Digital India to drive the digital economy to $1 trillion by 2025: Amitabh Kant. *Available at* https://www.digitalindia.gov.in/content/digital-india-drive-digital-economy-1-trillion-2025-amitabh-kant

3 Digital India. *Available at* https://www.digitalindia.gov.in/

4 *Ibid*

5 Impact of Criminalising Provisions on Ease of Doing Digital Business in India. *Available at* https://cuts-ccier.org/pdf/dp-impact-of-criminalising-provisions-on-ease-of-doing-digital-business-in-india.pdf

6 Impact of Regulatory Uncertainty on Ease of Doing Digital Business in India. *Available at* https://cuts-ccier.org/pdf/dp-impact_of_regulatory_uncertainty_on_ease_of_doing_digital_business.pdf

7 Budget allocation for Digital India programme increases by 67% for 2022-23. *Available at* https://www.thehindubusinessline.com/economy/budget/budget-allocation-for-digital-india-programme-increases-by-67-for-2022-23/article64963895.ece#:~:text=The%20Ministry%20of%20Electronics%20and,%E2%82%B96%2C388%20crores%20last%20year.

8 Study on the effect of the digital economy on high-quality economic development in China. *Available at* https://doi.org/10.1371/journal.pone.0257365

9 Vision and Vision Areas. *Available at* https://www.digitalindia.gov.in/content/vision-and-vision-areas

10 Access (In)Equality Index (AEI) Measuring (In)Equality of Access to Basic Opportunities Across India. *Available at* https://jgu.s3.ap-south-1.amazonaws.com/jslh/Access+(In)Equality+Index+Report+2021.pdf

11 The economic impact of broadband and digitization through the COVID-19 pandemic Econometric modelling. *Available at* https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.COV_ECO_IMPACT_B-2021-PDF-E.pdf

12 *Ibid*

13 Study on the effect of the digital economy on high-quality economic development in China. *Available at* https://doi.org/10.1371/journal.pone.0257365

14 Study on the effect of the digital economy on high-quality economic development in China. *Available at* https://doi.org/10.1371/journal.pone.0257365

15 India's new digital rules are bad news for democracy. *Available at* https://indianexpress.com/article/opinion/columns/social-media-rules-whatsapp-twitter-facebook-ott-platform-content-modi-govt-7213191/

16 Aryan cabs: leveraging it for rural connectivity. *Available at* https://www.researchgate.net/publication/335981299_Aryan_cabs_leveraging_it_for_rural_connectivity

17 *Ibid*

18 Internet penetration rate across India between January and November 2019, by state. *Available at* https://www.statista.com/statistics/1115129/india-internet-penetration-by-state/

19 Aryan cabs: leveraging it for rural connectivity. *Available at* https://www.researchgate.net/publication/335981299_Aryan_cabs_leveraging_it_for_rural_connectivity

20 [Startup Bharat] Weak internet infrastructure slowing the growth of J&K startup ecosystem. *Available at* https://yourstory.com/2020/05/startup-bharat-weak-internet-infrastructure-disrupt-jammu-kashmir-startup-ecosystem/amp

21 Access (In)Equality Index (AEI) Measuring (In)Equality of Access to Basic Opportunities Across India. *Available at* https://jgu.s3.ap-south-1.amazonaws.com/jslh/Access+(In)Equality+Index+Report+2021.pdf

22 Internet penetration rate across India between January and November 2019, by state. *Available at* https://www.statista.com/statistics/1115129/india-internet-penetration-by-state/

23 Tilt among micro and small enterprises to digital channels for sales. *Available at* https://www.crisil.com/en/home/our-analysis/reports/2020/12/tilt-among-micro-and-small-enterprises-to-digital-channels-for-sales.html

[24] What Needs to Be Done to Strengthen MSMEs, the Economy's 'Backbone'. *Available at* https://www.businesstoday.in/magazine/30th-anniversary-special/story/what-needs-to-be-done-to-strengthen-msmes-the-economys-backbone-321698-2022-02-17

[25] MSMEs Go Digital. *Available at* https://icrier.org/pdf/MSMEs_Go_Digital.pdf

[26] *Ibid*

[27] 6 Years of Digital India: How successful has PM Modi's plan been? *Available at* https://www.orfonline.org/research/6-years-of-digital-india-how-successful-has-pm-modis-plan-been/

[28] *Ibid*

[29] *Ibid*

[30] BharatNet: Digital India's biggest miss. The Deccan Herald. *Available at* https://www.deccanherald.com/specials/insight/bharatnet-digital-indias-biggest-miss-1015076.html

[31] *Ibid*

[32] *Ibid*

[33] India's gendered digital divide: How the absence of digital access is leaving women behind. *Available at* https://www.orfonline.org/expert-speak/indias-gendered-digital-divide/

[34] BharatNet: Digital India's biggest miss. The Deccan Herald. *Available at* https://www.deccanherald.com/specials/insight/bharatnet-digital-indias-biggest-miss-1015076.html

[35] *Ibid*

[36] 6 Years of Digital India: How successful has PM Modi's plan been? Observer Research Foundation. *Available at* https://www.orfonline.org/research/6-years-of-digital-india-how-successful-has-pm-modis-plan-been/

[37] BharatNet: Digital India's biggest miss. The Deccan Herald. *Available at* https://www.deccanherald.com/specials/insight/bharatnet-digital-indias-biggest-miss-1015076.html

[38] *Ibid*

[39] *Ibid*

[40] Why India must take the first step towards 5G rollout this year. *Available at* https://economictimes.indiatimes.com/industry/telecom/telecom-policy/why-india-must-take-first-step-towards-5g-rollout-this-year/articleshow/88643748.cms

[41] Trai's paper on using street furniture for 5G infra. *Available at* https://www.financialexpress.com/industry/trais-paper-on-using-street-furniture-for-5g-infra/2470145/

[42] Telcos get six-month 5G trial extension, spectrum auction likely delayed. *Available at* https://economictimes.indiatimes.com/industry/telecom/telecom-news/telcos-get-six-month-5g-trial-extension-spectrum-auction-likely-delayed/articleshow/87623902.cms

[43] India's tryst with 5G networks may get delayed - here's why. *Available at* https://www.techradar.com/in/news/indias-tryst-with-5g-networks-may-get-delayed-heres-why

[44] PM WANI. *Available at* https://dot.gov.in/pm-wani

[45] The PM-WANI Scheme: An Explainer. *Available at* https://internetfreedom.in/pm-wani-explainer/

[46] *Ibid*

[47] Wi-Fi ACCESS NETWORK INTERFACE (WANI) and Framework and Guidelines for Registration. *Available at* https://dot.gov.in/sites/default/files/2020_12_11%20WANI%20Framework%20Guidelines.pdf

[48] *Ibid*

[49] KYC registering agency gets cyber vulnerability alert. *Available at* https://indianexpress.com/article/india/no-data-breach-kyc-registering-agency-gets-cyber-vulnerability-alert-7594319/

[50] The PM-WANI Scheme: An Explainer. *Available at* https://internetfreedom.in/pm-wani-explainer/

[51] Wi-Fi ACCESS NETWORK INTERFACE (WANI) and Framework and Guidelines for Registration. *Available at* https://dot.gov.in/sites/default/files/2020_12_11%20WANI%20Framework%20Guidelines.pdf

[52] *Ibid*

[53] *Ibid*

[54] Explained | Right to be forgotten: govt position, court rulings, and laws elsewhere. *Available at* https://indianexpress.com/article/explained/explained-right-to-be-forgotten-7691766/

[55] *Ibid*

[56] Rajasthan to get high-speed internet connectivity, first state to install L-route server. *Available at* https://www.hindustantimes.com/india-news/rajasthan-to-get-high-speed-internet-connectivity-first-state-to-install-l-route-server-101650307273167.html

[57] *Ibid*

[58] *Ibid*

[59] UP govt orders to provide reliable Internet connectivity in villages. *Available at* https://www.hindustantimes.com/cities/lucknow-news/up-govt-orders-to-provide-reliable-internet-connectivity-in-villages-101651773844703.html

[60] Kerala: Select BPL families to get free internet by May-end. *Available at* https://timesofindia.indiatimes.com/city/thiruvananthapuram/kerala-select-bpl-families-to-get-free-internet-by-may-end/articleshow/91410607.cms

[61] *Ibid*

[62] *Ibid*

[63] Access to the internet is not a Fundamental Right. The Statesman. *Available at* https://www.thestatesman.com/supplements/law/access-internet-not-fundamental-right-1502893356.html

[64] Is the Internet a fundamental right? The contrasting stands of Centre and Kerala govt. *Available at* https://www.thenewsminute.com/article/internet-fundamental-right-contrasting-stands-centre-and-kerala-govt-117711

[65] India's Shutdown Numbers. Available at https://internetshutdowns.in/

[66] $3.04 billion has been lost due to internet shutdowns in the last five years: Report. *Available at* https://www.livemint.com/Industry/QDygwg5eRw1AkMavKvAfpK/304-billion-has-been-lost-due-to-internet-shutdowns-in-las.html

[67] Government Internet Shutdowns Have Cost Over $20 Billion Since 2019. *Available at* https://www.top10vpn.com/research/cost-of-internet-shutdowns/#india

[68] A year without high-speed internet ravaged health, education, entrepreneurship in Kashmir. *Available at* https://scroll.in/article/968719/a-year-without-high-speed-internet-ravaged-health-education-entrepreneurship-in-kashmir

[69] [Startup Bharat] Weak internet infrastructure slowing the growth of J&K startup ecosystem. *Available at* https://yourstory.com/2020/05/startup-bharat-weak-internet-infrastructure-disrupt-jammu-kashmir-startup-ecosystem/

[70] A year without high-speed internet ravaged health, education, entrepreneurship in Kashmir. *Available at* https://scroll.in/article/968719/a-year-without-high-speed-internet-ravaged-health-education-entrepreneurship-in-kashmir

[71] [Startup Bharat] Weak internet infrastructure slowing the growth of J&K startup ecosystem. *Available at* https://yourstory.com/2020/05/startup-bharat-weak-internet-infrastructure-disrupt-jammu-kashmir-startup-ecosystem

[72] Kashmir economy suffered loss of Rs 17,878 crore in 4 months after abrogation of Article 370. *Available at* https://www.news18.com/news/india/kashmireconomy-suffered-loss-of-rs-17878-crore-in-4-months-after-abrogatin-of-article-370-2428417.html

[73] Indian mobile carriers losing ₹ 2.4 cr revenue every hour owing to internet shutdowns. *Available at* https://www.livemint.com/industry/telecom/indian-mobile-carriers-losing-rs-2-4-cr-revenue-everyhour-owing-to-internet-shutdowns-11577460131477.html

[74] Between Rights and Risks: Life and Liberty In An Internet Dark Kashmir. *Available at* https://www.defindia.org/wp-content/uploads/2020/10/kashmir-longest-internet-shutdown.pdf

[75] [Startup Bharat] Weak internet infrastructure slowing the growth of J&K startup ecosystem. *Available at* https://yourstory.com/2020/05/startup-bharat-weak-internet-infrastructure-disrupt-jammu-kashmir-startup-ecosystem/

[76] 70 Percent of Global Internet Shutdowns in 2020 were India: Report. Times of India. *Available at* https://timesofindia.indiatimes.com/india/70-of-global-internet-shutdowns-in-2020-were-in-india-report/articleshow/81321980.cms

[77] Bhasin v Union of India. Global Freedom of Expression. *Available at* https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india

[78] *Ibid*

[79] *Ibid*

[80] *Ibid*

[81] India's Shutdown Numbers. *Available at* https://internetshutdowns.in/

[82] *Ibid*

[83] Calcutta HC stays internet shutdown issued by West Bengal Government. *Available at* https://internetfreedom.in/calcutta-hc-stays-internet-shutdown-issued-by-west-bengal-government/

[84] Internet Blocked In Jodhpur For Unspecified Amount Of Time. *Available at* https://www.medianama.com/2022/05/223-internet-shutdown-jodhpur-rajasthan/

[85] Exclusive: What Stands Out Among Internet Shutdowns Ordered In Meghalaya Since 2020? *Available at* https://www.medianama.com/2022/04/223-internet-shutdowns-meghalaya-reason-repeated-rti/

[86] Payments data must be stored in systems located in India, says RBI. *Available at* https://www.business-standard.com/article/economy-policy/payments-data-must-be-stored-in-systems-located-in-india-says-rbi-119062700043_1.html

[87] Number of internet users in EU countries as of December 2020. *Available at* https://www.statista.com/statistics/252753/number-of-internet-users-eu-countries/

[88] Data Centre Firms Ramp Up Capacity In India. Available at https://www.livemint.com/technology/tech-news/data-centre-firms-ramp-up-capacity-in-india-11640332271873.html

[89] Number of data centers in Europe by country 2021. *Available at* https://www.statista.com/statistics/878621/european-data-centers-by-country/

[90] Number of internet users in EU countries as of December 2020. *Available at* https://www.statista.com/statistics/252753/number-of-internet-users-eu-countries/

[91] Recommendations for Data Centre Policy. *Available at* https://community.nasscom.in/sites/default/files/report/25264-nasscom-recommendations-data-centre-policy.pdf

[92] What Is a Hyperscale Data Center? *Available at* https://www.vertiv.com/en-in/about/news-and-insights/articles/educational-articles/what-is-a-hyperscale-data-center/

[93] Recommendations for Data Centre Policy. *Available at* https://community.nasscom.in/sites/default/files/report/25264-nasscom-recommendations-data-centre-policy.pdf

[94] Budget 2022: 'Infra status to data centres may spur Rs 70,000-72,000 crore investments over five-ten years'. *Available at* https://economictimes.indiatimes.com/tech/technology/infra-status-to-data-centers-may-spur-rs-70000-72000-crore-investments-over-five-ten-years/articleshow/89275900.cms?from=mdr

[95] Data Centre Policy 2020. *Available at* https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf

[96] *Ibid*

[97] Comments for Ministry of Electronics & Information Technology (e-Governance Division) on Draft Data Centre Policy, 2020. *Available at* https://cuts-ccier.org/pdf/comments-for-ministry-of-electronics-and-information-technology-on-draft-data-centre-policy-2020.pdf

[98] Special economic zones — Major challenges: Multiple models, unutilised land and additional taxes. *Available at* https://indianexpress.com/article/business/business-others/major-challenges-in-special-economic-zones-multiple-models-unutilised-land-and-additional-taxes-5000292/

[99] Why mega food parks are failing to attract corporate interest. *Available at* https://www.businesstoday.in/magazine/features/story/food-parks-in-india-fail-to-attract-corporate-investment-48328-2015-06-24

[100] 12 startups from #BuildonIndiaStack venture pitch that are leveraging IndiaStack. *Available at* https://yourstory.com/2017/08/startups-buildonindiastack-venture-pitch-indiastack/amp

[101] The digital dream: Upskilling India for the future. *Available at* https://www.ideasforindia.in/topics/governance/the-digital-dream-upskilling-india-for-the-future.html.

[102] *Ibid*

[103] *Ibid*

[104] *Ibid*

[105] Review: Government's Digital Literacy targets not met because of paucity of funds. *Available at* https://factly.in/review-governments-digital-literacy-targets-not-met-because-of-paucity-of-funds/

[106] International Literacy Day: Bridging India's Digital Divide. *Available at* https://www.bqprime.com/technology/international-literacy-day-bridging-indias-digital-divide

[107] Review: Government's Digital Literacy targets not met because of paucity of funds. *Available at* https://factly.in/review-governments-digital-literacy-targets-not-met-because-of-paucity-of-funds/

[108] E-Commerce and Consumer Protection in India: The Emerging Trend. *Available at* https://link.springer.com/article/10.1007/s10551-021-04884-3

[109] *Ibid*

[110] *Ibid*

[111] *Ibid*

[112] *Ibid*

[113] 2 in 3 Indian SMBs suffered over Rs 3.5 crore business loss in post-pandemic cyber attacks: Survey. *Available at* https://www.financialexpress.com/industry/sme/msme-tech-2-in-3-indian-smbs-suffered-over-rs-3-5-crore-business-loss-in-post-pandemic-cyber-attacks-survey/2338676/

[114] *Ibid*

[115] How much does a data breach cost? *Available at* https://www.ibm.com/in-en/security/data-breach

[116] Number of internet users in India from 2010 to 2020, with estimates until 2040. *Available at* https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

[117] India to have 900 million active internet users by 2025, says report. *Available at* https://economictimes.indiatimes.com/tech/technology/india-to-have-900-million-active-internet-users-by-2025-says-report/articleshow/83200683.cms

[118] Cybersecurity Challenges for Indian MSMEs. *Available at* https://cuts-crc.org/pdf/briefing-paper-cybersecurity-challenges-for-indian-msmes.pdf

[119] The invisible hole of information on SMB's cybersecurity. *Available at* http://www.iiakm.org/ojakm/articles/2019/volume7_1/OJAKM_Volume7_1pp14-26.pdf

[120] *Ibid*

[121] National Cyber Security Strategy 2021 Draft Formulated By NSCS: Rajeev Chandrasekhar. *Available at* https://www.outlookindia.com/national/national-cyber-security-strategy-2021-draft-formulated-by-nscs-rajeev-chandrasekhar-news-189571

[122] *Ibid*

[123] *Ibid*

[124] Flag cyber incidents within six hours of detection, govt tells companies. *Available at* https://www.livemint.com/

[125] *Ibid*

[126] Exclusive: NordVPN may pull servers from India following the IT Ministry order. *Available at* https://entrackr.com/2022/05/exclusive-nord-vpn-may-pull-servers-from-india-following-it-ministry-order/

[127] Can India Address the Growing Cybersecurity Challenges in the Nuclear Domain? *Available at* https://www.orfonline.org/research/can-india-address-the-growing-cybersecurity-challenges-in-the-nuclear-domain/

[128] *Ibid*

[129] *Ibid*

[130] India in final stages of clearing national cybersecurity strategy. Business Standard. *Available at* https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cybersecurity-strategy-121102700663_1.html

[131] India Stack. *Available at* https://indiastack.org/

[132] India's Approach to Open Banking: Some Implications for Financial Inclusion. *Available at* https://www.imf.org/-/media/Files/Publications/WP/2021/English/wpiea2021052-print-pdf.ashx

[133] Big Data in India: Benefits, Harms, and Human Rights - Workshop Report. *Available at* https://cis-india.org/internet-governance/big-data-in-india-benefits-harms-and-human-rights-a-report#7

[134] OpenPDS: Protecting the Privacy of Metadata through SafeAnswers. *Available at* https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0098790

[135] Big Data in India: Benefits, Harms, and Human Rights - Workshop Report. *Available at* https://cis-india.org/internet-governance/big-data-in-india-benefits-harms-and-human-rights-a-report#7

[136] Digital Economy & Digital Payment Division (DEDPD). *Available at* https://www.meity.gov.in/digidhan

[137] Digital payments to touch USD 1 tln by 2026: CLSA. *Available at* https://www.cmie.com/kommon/bin/sr.php?kall=warticle&dt=20211217123706&msec=310

[138] The Future of Disruptive and Enabling Financial Technology post CV-19. *Available at* https://ee911a6f-cb33-467b-961a-87b9cafb2752.filesusr.com/ugd/14138f_ea533f6e680b46b3af3d1b0aa7f8d10d.pdf

[139] Digital Payments 2020. *Available at* http://image-src.bcg.com/BCG_COM/BCG-Google%20Digital%20Payments%202020-July%202016_t

[140] India shows the world how to take 1.3 billion people to the bank. *Available at* https://theprint.in/economy/india-shows-the-world-how-to-take-1-3-billion-people-to-the-bank/621069/

[141] Aadhaar 2.0: Creating India's digital infrastructure *Available at* https://www.livemint.com/Politics/afjuy0dHgS4beFggSTVddP/Aadhaar-20-Creating-Indias-digital-infrastructure.html

[142] India's Approach to Open Banking: Some Implications for Financial Inclusion. *Available at* https://www.imf.org/-/media/Files/Publications/WP/2021/English/wpiea2021052-print-pdf.ashx

[143] Explained: Everything you need to know about RBI's Payments Infrastructure Development Fund. *Available at* https://www.moneycontrol.com/news/business/explained-everything-you-need-to-know-about-rbis-payments-infrastructure-development-fund-6317541.html

[144] Digital Payments in India to grow to 71.7% of all payment transactions by 2025: Report. *Available at* https://www.thehindubusinessline.com/news/digital-payments-in-india-to-grow-to-717-of-all-payment-transactions-by-2025-report/article34204827.ece

[145] Can ONDC overcome UPI's challenges? *Available at* https://analyticsindiamag.com/can-ondc-overcome-upis-challenges/

[146] 'Despite privacy concerns, consumers big on digital payments this festival season' *Available at* https://www.thehindubusinessline.com/money-and-banking/despite-privacy-concerns-consumers-using-digital-payments-in-a-big-way-for-festival-shopping-study/article29775378.ece

[147] Privacy and security risks of digital payments. *Available at* https://www.orfonline.org/research/privacy-security-risks-digital-payments/

[148] Paytm Mall suffers massive data breach, ransom demanded: Report. *Available at* https://economictimes.indiatimes.com/tech/internet/paytm-mall-suffers-massive-breach-ransom-demanded-report/articleshow/77833664.cms

[149] Strategy for National Open Digital Ecosystems (NODE) Whitepaper. *Available at* https://www.medianama.com/wp-content/uploads/mygov_15821931145155322 11.pdf

[150] *Ibid*

[151] *Ibid*

[152] *Ibid*

[153] *Ibid*

[154] CUTS Submission to the Ministry of Electronics and Information Technology on Strategy for National Open Digital Ecosystems. *Available at* https://cuts-ccier.org/pdf/submission-to-ministry-of-electronics-and-information-technology-on-strategy-for-national-open-digital-ecosystems.pdf

[155] Government clears policy to sell vehicle registration data. A*vailable at* https://www.hindustantimes.com/delhi-news/govt-clears-policy-to-sell-vehicle-registration-data/story-n4aBtGpJgETNuN9vbAW3LL.html

[156] Explained: Why ONDC push could boost small retailers online. *Available at* https://indianexpress.com/article/explained/open-network-for-digital-commerce-small-retailers-7899437/

[157] Open Network for Digital Commerce: Democratising Digital Commerce in India. *Available at* https://www.medianama.com/wp-content/uploads/2022/03/ONDCStrategyPaper.pdf

[158] *Ibid*

[159] Can ONDC overcome UPI's challenges? *Available at* https://analyticsindiamag.com/can-ondc-overcome-upis-challenges/

[160] *Ibid*

[161] Digital India dream and arbitrary internet shutdowns can't go together. Just see the loss. *Available at* https://theprint.in/opinion/digital-india-dream-and-arbitrary-internet-shutdowns-cant-go-together-just-see-the-loss/884234/

[162] *Ibid*

[163] *Ibid*

[164] *Ibid*

8
CHAPTER

Impact of Barriers on Cross-Border Data Flow on the Ease of Doing Digital Business in India

Asheef Iqubbal, Senior Research Associate, CUTS International

Overview

Data-driven services have accelerated economic inequality within and across the country which has led to calls for restrictive measures in cross-border data flows globally.[1] However, their impact on containing inequality remains unclear. India is also deliberating moving towards data localisation, an idea rooted in the concept of *data sovereignty*[2] that puts conditions and/or restricts data flow across national boundaries and mandates data storage within the national border.[3]

In multiple draft documents such as the draft E-Commerce Policy, draft Non-Personal Data Governance[4], proposed Data Protection Bill, 2021,[5] and Reserve Bank of India (RBI) Notification on Storage of Payment System Data, the Indian government has shown a clear intent of mandating the storage of data within national boundaries. This is being done to boost the domestic digital economy and businesses, enhancing security and privacy and strengthening law enforcement mechanisms.[6]

However, restrictive measures on data flow might lead to the fragmentation of the digital ecosystem, hampering the growing realisation of a globally connected digital economy. One of the issues stemming from data localisation mandates – increasing barriers to cross-border data flow – poses a critical concern to the future of international trade and digital businesses globally as it erects borders in cyberspace. The fundamental tenet of the Internet – free, decentralised, and open network – has brought many economic benefits.

This discussion paper, under the *Ease of Doing Digital Business (EoDDB) in India* study,[7] analyses the impact of restrictions on cross-border data flows on doing digital businesses by identifying bottlenecks such as an increase in compliance, regulatory uncertainty, and inadequate infrastructure for the firms operating in multiple jurisdictions. To this end, the paper recommends mechanisms for strengthening cross-border data flow with adequate security and privacy measures for policymakers, businesses, and authorities to consider.

Introduction

Technology-led economic growth has not only accelerated economic inequality within and across countries but also opened a deep fault line in terms of surveillance and law enforcement. According to United Nations Conference on Trade and Development's (UNCTAD's) report on digital economy estimates,[8] the United States (US) and China hold 90 percent of the capitalisation of the top 70 digital platforms globally. Digital corporations have strongly benefited globally from accelerated digitalisation needs due to COVID-19.[9]

Concerns related to the concentration of wealth, power, threats to privacy, and security are pushing nations to recalibrate their digital

Concerns related to the concentration of wealth, power, threats to privacy, and security are pushing nations to recalibrate their digital governance mechanisms, particularly the flow of data across borders.

governance mechanisms, particularly the flow of data across borders. By mandating storage of data within national boundaries, the strategy of governments appears to be aimed at exerting more control over the digital ecosystem, particularly restricting the influence and domination of Big Tech. Governments claim that it will help in enhancing security, law and enforcement mechanisms, employment generation, and boosting the digital economy in the country through state control over data, data flows, and digital technologies.[10]

As governments around the world are starting to recognise the value of data and its commercial use, countries are increasingly mandating regulations that restrict the flow of data across borders.[11]

Restriction on cross-border data flows targets a growing range of specific data types that can be broadly categorised as data deemed "important" or "sensitive" or related to national security. The restrictions are being mandated through data localisation policies which can be described as an idea grounded in the concept of data sovereignty where restrictions are imposed on the cross-border transfer of data and are mandated to be stored within the country.[12]

Data localisation can be mandated in multiple forms such as the complete prohibition of transfer of data, allowing transfer after obtaining requisite permissions, storing mirrored copies of data within national boundaries, and taxation on transfer. Policies that restrict the flow of data include blocking the transfer of data across borders, which is also known as *hard data localisation,* or putting conditions on the data flows, storage, and processing which has been termed as *soft data localisation*.[13]

35 countries had implemented 67 restrictive measures – both soft and hard – in 2017. In 2021, 62 countries have put 144 restrictions on data flowing across the border.[14] However, it remains ambiguous how the objectives of restricting cross-border data flow will be effectively met. As a consequence of these restrictive measures that intend to regulate cross-border data flows, an open, rules-based, and innovative global digital economy is facing a growing threat. An Information Technology and Innovation Foundation (ITIF) study[15] found that a one-point increase in a nation's data restrictiveness cuts its gross trade output by 7 percent and slows its productivity by 2.9 percent, and hikes downstream prices by 1.5 percent over five years. This is because many countries are enacting barriers to cross-border data flow that make transferring data across borders more expensive and time-consuming. The flow of data across borders is fundamental for decision-making in digitally-enabled business models as businesses use data to create value and maximise that value.[16]

India already has regulations under implementation and has also proposed policies that mandate degrees of restrictions on the cross-border flow of data. In multiple recent policy documents such as the draft E-Commerce Policy, draft Non-Personal Data Governance, and the proposed Data Protection Bill, 2021, the Government of India (GoI) makes it clear that India is fast moving towards restriction on cross-border data flow. Reserve Bank of India's (RBI's) Notification on the Storage of Payment System Data also points in the same direction.

Key considerations for mandating and/or proposing data localisation policies are fostering better economic growth and enhancing security. However, GoI has not backed the restriction on cross-border data flow with clear evidence as to how it will strengthen security and the growth of the digital economy. Researchers have warned that it is unlikely to enhance security as the security of data is not dependent on the data storage location.[17] Instead, the security of data is highly dependent on the company's security guidelines, framework used for data protection, and technical capability and they are usually uniform across the globe.

The cost-benefit analysis also needs to be taken into account while formulating policies.[18] In this context, policies that restrict cross-border data flow must be evaluated on how well they are aligned with the intended aims and their implications for the digital economy. While multiple aspects of data localisation have been debated and continue to generate significant attention, the scope of this paper will be limited to its impact on doing digital business in India, particularly focusing on small and medium businesses.

The first section of the paper situates India's data localisation move in the broader global discourse as it cannot be understood in isolation. The second section of this paper provides the impact of proposed data localisation in the context of the proposed Data Protection Bill, 2021.

The second section deals with RBI Notification on data storage within India and its impact on the financial sector. The third section deals with the proposed data localisation mandates under the IT Act of 2000 and its impact on digital businesses. Based on the analysis, the final section combines recommendations relating to mechanisms to support data flows, global digital trade and data governance.

Situating India's Data Localisation Debate in Global Discourse

As of 2022, worldwide internet networks are carrying 46.6 terabytes of data per second as compared to 100 gigabytes in 1992, which means an exponential increase in the generation of personal and non-personal data.[19]

The generation of huge amounts of data and their cross-border flow has heavily contributed to the growth of data-driven enterprises globally, as it allows better coordination, efficiency, and delivery of goods and services.[20]

With an increasingly central role and value of data in the global economy, the debate around storing data within the national boundary has gained significant attention.[21]

As a part of this debate, in India, like any other country, multiple sets of arguments have been put forth on the grounds of economy, security, and individual liberty, among others. Policymakers have argued that data localisation will boost national digital economies, enhance security, and better law enforcement mechanisms. The UNCTAD's 2021 Digital Economy Report also states there is an urgent need to adequately regulate cross-border data flow at the international level due its increasing economic value.[22]

GDPR creates hard localisation by laying out technical standards and requirements for handling personal information gathered in its member states and strictly restricting data transfers to "unsafe" geographies.

However, data localisation poses a significant challenge such as transnational regulatory tension. For example, the idea of adequacy, adopted by the European Union in the General Data Protection Regulation (GDPR) to flow data outside the European nations, is increasingly being espoused by multiple countries, including India. However, there is a lack of uniformity in terms of equivalent standard restrictions, consent restrictions, no transfer rules, and mirror copy, creating a bottleneck in the seamless flow of data.[23]

GDPR creates hard localisation by laying out technical standards and requirements for handling personal information gathered in its member states and strictly restricting data transfers to "unsafe" geographies. Indian proposed law mandates the physical presence of data and/or copies within the country while countries such as China and Russia mandated additional localisation requirements including reviews of source code and restrictions on cryptography. In addition, countries such as Indonesia, Malaysia, and India have proposed to put conditional requirements on the transfer of non-personal data as well.[24]

Since regulations are still evolving and expanding, it creates uncertainty among digital businesses, adding to the challenges of updating their approaches. This is particularly challenging as these approaches often require reprogramming of technological specifications. Multiple countries such as the ones in West Asia are mandating companies to build digital infrastructure in their countries. These requirements will be difficult and resource-intensive for digital businesses to negotiate and comply with specific guidelines for technology decisions.[25]

Businesses are not only dealing with consumer privacy but also with laws in multiple jurisdictions that put the responsibility for consumer privacy even in foreign jurisdictions. Digital platforms will find it difficult to safeguard consumers' privacy in the context of data stored in different jurisdictions.[26]

Companies are still learning to negotiate with requirements such as "equivalent standards" of GDPR. For example, the recent Schrems II decision in Europe has put restrictions on third-country personal data transfers to countries that are not currently on the European Commission's adequacy list. As a result of this, multiple companies adopted Standard Contractual Clauses (SSC) rather than Safe Harbor, which was earlier used to make a case for an adequate level of protection.

The Court of Justice of the European Union (CJEU) ruled that the 'EU-US Privacy Shield' does not provide adequate protection, therefore, is no longer valid for transferring data from the EU to the United States of America (USA). This is because US laws do not provide data subjects 'actionable rights before the courts against their authorities. The CJEU ruled that SSC remains valid, but on its own may not be enough to ensure an adequate level of protection.

Personal data can only be transferred if the importer and the exporter can ensure that the protection set out in the SCCs can be complied with in practice. This will also impact Indian companies providing digital services in the EU and processing data in India. India now provides a basic framework for data protection but needs to straighten proposed data protection mandates.

The data localisation debate has also been mired with its impact on digital trade in terms of how it will be enforced and its impact on trade agreements. The debate around data-driven economic growth has furthered the realisation of global interdependencies through the cross-border data flow. However, this has been unequally distributed. Developing countries have not been able to gain adequate benefits from the data generated domestically due to infrastructural and technical constraints.

In the absence of an optimal global alliance to maintain data-driven services, the question of data sovereignty and distribution of wealth was inevitable. The US has been at the forefront of the increasing data sovereignty approach. USA's Securities and Exchange Commission (SEC) has stated that "some countries, such as India, are considering or have passed legislation implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our (firms based in the USA) services."[27]

While the General Agreement on Trade in Services (GATS), under World Trade Organisation (WTO), does not explicitly prohibit data localisation measures, there is increasing pressure to include localisation as a trade-restrictive measure.[28]

In light of increasing data localisation, more and more countries are willing to accept the free flow of data in their regional and bilateral trade agreements. A major international initiative on data flows, the Osaka Track, was launched by heads of government under Japan's G20 leadership in 2019.[29]

'Data free flow with trust (DFFT)' to increase trust and openness in data flows co-exist and complement each other. In parallel, 76 countries launched new negotiations on digital trade in the Joint Statement Initiative (JSI) on e-commerce. The Group of Seven's (G7's) 'G7 Digital and Technology Ministers' meeting in April 2021 also discussed cooperation on Data Free Flow with Trust.[30]

These initiatives have raised multiple concerns in developing countries as it does little to quell developing countries' economic concerns. India has taken an oppositional view on the unhindered free flow of data, which the Indian government believes fails to account for emerging economies' developmental interests. At international forums, India has been a vocal critic of the free flow of data across borders due to its assertion as a developing country and stated priorities of developing policy by taking into account domestic concerns and interests.

Subsequently, India did not participate in the Osaka track for DFFT and WTO negotiation on e-commerce and is even hesitant to accept it due to its apprehensions about unequal treatment of data.[31] As India assumes the presidency of G20, developing countries and MSMEs will be hoping that their needs and concerns will be considered when discussing cross border flow of data.

Impact of Barriers on Cross-Border Data Flow on Ease of Doing Digital Business

Box 1: Draft Data Protection Bill 2021

In India, the conversation around data protection started primarily in 2017 after the Supreme Court of India declared privacy as a fundamental right protected under the Indian constitution. This was pronounced in Justice K.S. Puttaswamy v. Union of India which resulted in PDP '19. After two years of deliberation and consultation with relevant stakeholders around personal data protection, in 2021, the Joint Parliamentary Committee (JPC) tabled its report on the Personal Data Protection Bill, 2019.[32]

The JPC notes that data localisation will help enhance security, law, enforcement, and employment generation and boost the digital economy.[33] Along with multiple substantive changes including in data localisation norms, the JPC proposed changing the name of the draft bill to Data Protection Bill, 2021 (DPB '21).

The latest draft bill repeatedly argues for making data generated in India available to Indian firms. The draft bill views it as an enabling force for homegrown digital businesses to participate in the digital economy. The JPC has suggested developing gradual data localisation, aiming to enhance security and boost the country's digital economy grounded in national sovereignty, including developing adequate technical infrastructures, taxation of the data flow, and introducing alternate payment methods.[34]

The latest draft bill categorises personal data into critical personal data (CPD) and sensitive personal data (SPD).[35] Herein, the JPC proposes to mandate that a copy of CPD and SPD stored in different jurisdictions must be brought back and stored within the country in a time-bound manner.

In addition to this, the latest draft of the bill empowers the government to expand the scope of SPD under Section 15.[36]

However, CPD is yet to be defined and is left to the government for open interpretation. The JPC states that taking SPD outside of Indian borders will require approval from the Data Protection Authority (DPA) which will be in consultation with the Central Government as well as the approval of the data principal will be required. The proposed mandates also stated that the Central Government and DPA can reject the data transfer if it is not in line with the public policy or state policy. The requirement of approval includes an intergroup scheme as well. These mechanisms are being introduced to curb the "potential misuse of the provision by individuals or organisations with mala fide intentions or by foreign entities whose actions might be inimical to the interests of the State".[37]

Moreover, the JPC recommendation also mandates that SPD shall not be shared with any foreign government or agency without the approval of the Indian government to "safeguard the data of Indians and keep in view the shifting nature of international relations."[38]

Compounded with the limitations on the flow of SPD, CPD has not been allowed to be transferred outside the country, unless for a few narrow exceptions relating to emergency services or certain entities outside India after the approval by the Central Government. This can only be done by meeting adequate requirements and if the transfer of such data does not prejudicially affect the security and strategic interest of the country.[39]

After DPA and infrastructures for the data storage are established, the JPC recommends, "the Central Government must ensure that data localisation provisions under this legislation are followed in letter and spirit by all local and foreign entities and India must move towards data localisation gradually".[40]

The Indian government has repeatedly affirmed that storing data within national boundaries will boost the growth of locally grown start-ups and the data-driven economy in India. While the objectives of restricting cross-border data flow may be legitimate, it might be challenging for doing digital business in India, particularly for Micro, Small, and Medium Sized Enterprises (MSMEs). Indian MSMEs account for 6.11 percent of the country's Gross Domestic Product (GDP) and 24.63 percent of GDP from the services sector, largely driven by data. India is home to many promising smaller firms that are seeking to move beyond India's borders and restrictions on cross-border data flows might be disproportionately challenging for them.[41]

Currently, many MSMEs use cloud computing to store data across national servers. Requirements of storing data within national borders will inevitably increase initial and ongoing costs for both foreign as well as domestic digital businesses.[42] This is because local data services incur significant costs in terms of infrastructure, data migration, and data storage, without enjoying the same efficiencies.[43]

For example, a study in the context of GDPR shows that storing data within national borders might increase the cost of setting up servers in a country by 30-60 percent and MSMEs may not make enough profit to afford this extra cost imposed on them.[44]

Further, digital businesses require hyper-scale data centres that would ensure better access and analysis of large volumes of data which will add value to their supply chain and enhance customer experience by advancing levels of personalisation.[45]

There could be multiple reasons for firms to store their data across the servers, including quality, backup in case of software failure, balancing, and data sharding.[46] Despite some significant push, India currently lacks modern data centres.[47]

To function across national boundaries, technological firms would have to bear the costs of data storage and processing mechanisms in each jurisdiction as a capital investment and the recurring costs of building data-related infrastructure. Studies have shown that restrictions on cross-border data flow negatively impact innovation and the start-up ecosystem and their ability to participate in global business structures.[48]

Further, if India continues to move towards data localisation, there could be a response to it in terms of retaliatory measures from the world, which will negatively impact the ecosystem of the Indian digital economy. For instance, the contribution of the Information Technology-Business Process Management (IT-BPM) sector to India's GDP rose from 1.2 percent in 1998 to 10 percent in 2019, which is heavily dependent on favourable policies for cross-border data flows.[49]

if India continues to move towards data localisation, there could be a response to it in terms of retaliatory measures from the world, which will negatively impact the ecosystem of the Indian digital economy.

This growth has been achieved due to the flow of data across borders, as Indian firms work with multiple businesses that are operating in different parts of the world, and any retaliatory measures will lead to the potential breakdown of data flow. This will significantly harm the growth of the data-driven service sector in India. Notably, service sectors attract the Foreign Direct Investment (FDI) inflow, which brings associated benefits to it such as knowledge and technology. Further, digital services exports also enable opportunities for innovation and start-ups by enabling knowledge and data sharing and collaboration on research and development across all sectors.[50]

CUTS study 'Digital Trade & Data Localisation' shows the unintended consequence of data localisation on India's IT-BPM Industry under different conditions of restrictions. The conditions vary according to the restrictiveness of the measures and whether they are implemented by India, its major trading partners in retaliation, or by multiple governments. The scope and extent of data restrictiveness may plunge the digital services exports between 10 to 19 percent in India. This may translate to a shortfall of US$19-36bn in achieving the digital sector's US$1tn economic value potential in 2025. The decline in digital services export will negatively affect India's GDP by 0.18 to 0.35 percent, causing a shortfall of US$9-17bn in the US$5tn economy objective in 2025.[51]

Economic implications of restrictions on cross-border data flow are not limited to a loss in a relevant country's GDP but also spread out to a decline in exports, investment, productivity and income loss to

workers.[52] Given this, framing optimal policies for cross-border data flows would be crucial for the growth of the digital economy and associated sectors and, in turn, boost the country's GDP.

A one-size-fits-all policy for regulating cross-border data flows will make doing business for digital business difficult in general and innovation and start-up ecosystems, in particular. For instance, compliance costs are also estimated to have a significant negative impact on MSMEs.[53]

While bigger firms might be able to incur such costs, it would disproportionately harm the prospects of smaller firms, widening existing gaps in the equal playing field, and thus, exacerbating economic inequalities. Since larger firms will be able to afford the costs of localisation more than smaller players, some of them have been staunch supporters of the pro-localisation stance.[54]

Considering, competition for India's big digital businesses stems from foreign players seeking to enter the market, localisation has the potential of eliminating these foreign players, while also imposing additional compliance costs on smaller domestic players, at least in the short run. MSMEs handle CPD, so even data localisation for just this data subset could harm Indian digital businesses.

Restrictive measures in the flow of data across national boundaries might bottleneck particularly smaller ventures to access global consumers without developing and/or renting infrastructure to store data in multiple jurisdictions. This will limit firms' capacity to provide services abroad easily and their participation in a globalised business and commerce. In the context of the EU's restriction on cross-border data flow, a study found "around 65 percent of companies would need to either redesign their products or reengineer their processes. This increases to 87 percent among companies that share data intensively."[55]

Firms are likely to find data localisation requirements difficult, to provide their services to consumers, thus increasing costs and barriers to entry. Moreover, it problematises the creation of workable data sets as they are stored in multiple unfamiliar locations, thus leading to the creation of vulnerable points and increasing the fear of error, particularly in the context of data mirroring. It will be expensive and put smaller companies in a vulnerable position as they are likely to find it difficult to meet adequate requirements and resources.[56]

For instance, smaller service providers operating with limited resources may not be able to differentiate between SPD and CPD – as proposed by JPC – and be compelled to store entire personal data themselves in India. A substantial portion of SPD is being shared by data principals (users) with different data fiduciaries (service providers) while availing of various data-driven services.[57]

Examples include sharing financial data with ride-hailing apps, food delivery service providers, and e-commerce companies, among others. Because of costly requirements, many smaller businesses might not be able to mobilise resources in terms of legal and technical capabilities to manage data effectively. Research in the context of GDPR shows that due to limited technical and legal capability, smaller firms have discontinued operations or switched to less cost-effective service providers.[58]

Furthermore, requiring business firms to develop infrastructures and update and defend data storage across multiple jurisdictions would broaden the attack surface for malicious hackers.[59] Data stored in a single server within the national border prevents the sharing of data to identify IT system vulnerabilities and help firms detect and respond to cyberattacks and would fail to update vulnerable systems being lost via phishing attacks.[60]

Regardless of where the data is stored, data security depends on the service provider's technical, physical, and administrative controls, which can be either strong or weak. Data localisation will increase the data breach vulnerability. Maintaining the protocol for data security across national boundaries would not be easier for business firms, particularly training staff for the sensitive functioning of data security across multiple countries.[61]

Impact on Digital Financial Services

Box 2: RBI Data Localisation

The RBI Notification[62] mandates that all payment system providers should store payment data only in India. It includes end-to-end transaction details or any information collected, processed, or carried out as part of payment instructions. The RBI Notification allows for the processing of payment data outside India for 24 hours, however, after this deadline, all such data needs to be stored within India. This was later expanded after the National Payments Corporation of India updated its guidelines that third-party application providers such as Google Pay, and WhatsApp Payments should store all payment data in India.[63] RBI's prior approval is necessary for sharing the payment system data with overseas regulators.

All payment firms, including American Express, Master Card/Visa, PayPal, Google Pay, WhatsApp Pay, Paytm, and Phone Pe, should adhere to the RBI's data localisation rule and store data within India for supervisory purposes.[64]

Foreign legs of transactions may be processed offshore and financial crime compliance systems are not expected to be in the scope of RBI mandates. Along with this, banks are expected to use panel auditing firms to confirm their approach to dealing with payment data and compliance with the notice. However, any subsequent activity such as settlement processing after payment processing, if done outside India, shall also be undertaken/performed on a near real-time basis by storing it only in India.[65]

Over the past few years, India has been witnessing ongoing digital advancements in terms of innovation, infrastructure, and growth of data-driven services. These advancements propelled cashless transactions which are further fuelled by the COVID-19 pandemic. According to the Ministry of Electronics and Information Technology (MeitY), the volume of digital payments in India has increased by 33 percent. A total of 7,422 crore digital payment transactions were recorded during FY 2021-22, up from 5,554 crore transactions seen in FY 2020-21.[66]

There are several payment options available due to Unified Payments Interface (UPI), an open Application Programming Interface (API). Along with smaller financial service providers, major players such as Google Pay, Phone Pay, and PayPal have access to sensitive users' financial data stored across international servers. This raised critical issues regarding users' data security, privacy, and law enforcement.

Increasing data breaches and security concerns pushed RBI to undertake steps aiming to protect consumers' interests. Under the Payment and Settlement Systems Act, of 2007,[67] RBI issued a circular in 2018, stating that all authorised Payment System Operators (PSOs) in India will have to ensure that the data is stored only in India after the processing. This includes data related to payment sensitivity, payment credentials, transactions, end-to-end transaction details, or any information collected, processed, or carried out as part of payment instructions. RBI insisted on system providers for unfettered access for supervisory purposes to all data. Proponents of data localisation argue that it will allow governmental authorities to access customers' data more swiftly.[68]

Along with the development of local data centres by the payment service companies which will help in employment generation locally, it will also increase the physical presence of these companies in India, thus making them more accountable to the Indian authorities.[69]

The move forced multinational firms to comply with data localisation norms and set up data storage in India. This also led them to carry out processes like fraud monitoring and revenue assurance which were carried out outside India.[70] However, RBI's move raised questions as it did not consult with relevant stakeholders. Such measures can lead to policies without the understanding of potential consequences in terms of ease of doing digital business in India.[71]

As India's fintech ecosystem has begun its expansion outside the Indian territories, it would be critical to ensure these firms do not stand oppositional to the international norms in terms of data storage and

processing. It will also help India in elevating its leadership role for creative innovations in the sector. For instance, Google wrote to the US Federal Reserve to urge the regulator to build a real-time payments architecture on the lines of India's UPI.[72]

Different types of companies seem to be affected differently by the data localisation requirements of RBI. While big financial services platforms felt the disruption, start-ups and smaller firms felt the brunt to localise their data. With limited resources, smaller ones would find data localisation norms difficult and resource-intensive to comply with due to the requirement of infrastructure and resources to manage the data which will harm competition and innovation in the sector.[73]

Different types of companies seem to be affected differently by the data localisation requirements of RBI. While big financial services platforms felt the disruption, start-ups and smaller firms felt the brunt to localise their data. With limited resources, smaller ones would find data localisation norms difficult and resource-intensive to comply with due to the requirement of infrastructure and resources to manage the data which will harm competition and innovation in the sector.

Fintech start-ups' business models significantly rely on outsourcing technical support and cloud services to affordable service providers across borders. Because of data localisation, startups will not be allowed to select affordable cloud service providers from the global competitive standards. Along with this, storing data within the national borders will compel them to undertake product re-engineering based on intricate laws in different jurisdictions, raising technical and operational costs such as compliance. For instance, financial service provider firms have been arguing that data localisation could compromise their ability to detect fraud and money laundering in the domestic payments system.[74]

Real-time fraud and money laundering detection rely on noting unusual payment patterns across jurisdictions.[75]

In the context of data localisation, it will be difficult for financial services to implement and monitor uniform policies such as risk management due to varying legal requirements in each jurisdiction.[76]

Decentralised models divide management attention and the allocation of resources. To manage the risks, financial services providers require a comprehensive understanding of their consumers, therefore, routinely transferring data across locations.[77]

Regulations that mandate the localisation of data make it difficult to achieve these objectives, often resulting in complexity in doing digital business. Moreover, it will increase the cost of financial services as they have to create a separate infrastructure, computing capabilities, and teams for each jurisdiction. Further, it is still not clear how storing data within the national border enhances the security of data. For instance, in an international transaction, regulators will have only access to half of the data that occurred in their jurisdiction.[78]

However, this may turn into a conflict between involved authorities and legislation, thus, raising difficulty for financial services to navigate multiple jurisdictions. Due to these resource-intensive requirements, only large financial services can function in multiple jurisdictions, harming smaller businesses, startups, and innovations.

Multinational payment systems located in India faced a major impact after the RBI's data localisation. Towards the enforcement of the notification, the RBI, through two separate orders, barred American Express and Diners Club from onboarding new customers and issuing new cards after they failed to comply with the data storage requirements.[79]

Moreover, for foreign companies, such compliances are an additional cost to their existing investments in the country and make the ease of doing business complicated. WhatsApp Payments also faced regulatory blockage by the RBI for many years due to not complying with the payments data storage notification, thus affecting competition in the market, and consequently impacting innovation and quality of services.[80]

Similarly, RBI's mandate of storing data within the national boundary prevented Apple from launching its digital payments service, specifically designed for Apple devices in India.[81]

In 2021, RBI also restricted Mastercard from onboarding new customers and issuing new cards.[82] However, now RBI has lifted such restriction which allows Mastercard to issue new cards to customers in India. The restriction was placed in pursuance of RBI's data localisation requirements and led to strained relations of the corporation with card issuers such as banks that relied on it.[83]

Notably, many banks collaborate with Mastercard to issue debit and credit cards. For a brief period, the move impacted the operations of some banks in issuing debit and credit cards to new customers.[84]

Major financial companies expressed their discontent with data localisation in RBI's mandates, particularly in the context of RBI's directive on payment storage.[85] For instance, the Chief executive of Visa, a financial service company based in the USA, Alfred F Kelly Jr said, "there are countries like India who have decided that one of the ways to protect data is to localise it. I don't necessarily think that is necessarily the best answer."[86]

Implications of CERT-In Rules on EoDDB

Box 3: CERT-In Data Localisation

The Indian Computer Emergency Response Team (CERT-In) issued new directions under section 70B of the parent legislation, the Information Technology Act, 2000 (IT Act) on 28 April 2022.[87]

CERT-In directions mandated that all firms have to maintain logs for a rolling period of 180 days within India, effectively imposing data localisation. In addition to this, service providers will have to also maintain data related to subscribers in an accurate manner for 5 years. These data sets include subscriber names, period of hire including dates, IPs allotted and used, e-mail address along with IP and time stamp used at time of registration, the purpose of availing the services, verified address and contact numbers, and ownership pattern of subscribers. However, these directions raised concerns as a public consultation was not undertaken before publishing it.

Indian Computer Emergency Response Team (CERT-In) on April 28, 2022, under Section 70B of the Information Technology Act, 2000 ("Directions") issued directions [See Box 3]. The objectives of CERT-In directions are legitimate as it attempts to address critical issues that India has been increasingly facing—cybercrimes and compromise of data security. 1.4 million incidents in 2021 and 212,000 incidents in January and February of 2022 alone have been a matter of concern for regulators as it negatively impacts the digital business community, particularly MSMEs, as well as consumers.[88]

The average cost of a data breach in India is US$2.12mn and the average time to identify a data breach stood at 239 days and it takes 81 days to contain a data breach.[89] However, CERT-in directions have mandated requirements such as maintaining logs of all ICT systems for 180 days "within the Indian jurisdiction", effectively imposing data localisation. In addition to this, the directions also mandated that multiple service providers such as data centres, cloud, and virtual private networks will have to maintain details for 5 years.

Along with big service providers such as ExpressVPN and Surfshark, smaller firms have shown their discontent with data storage requirements within India's jurisdiction. They argued that this will impose onerous costs of data-related infrastructure and compliance burdens on doing digital in India, particularly putting MSMEs in a vulnerable position as they might not have the technical capability to report incidents and resources to build capacity.[90]

A Small and Medium-sized Enterprises (SME) group made a submission to MeitY and CERT-In asking for an extension on the time given to comply with the latter's Cybersecurity Directions to 300 days. The submission also seeks clarity on how CERT-In would secure the data it has collected, its data logging requirement, and so on.[91] The SME group during the consultation had claimed that the heavy costs of storing logs were prohibitive for SMEs as the cost involved is approximately US$1000 to US$2000 weekly for one Terabyte of data.[92] CERT-In has extended the deadline for MSMEs till September 25 to comply with its cybersecurity directions. For others, the directions became effective on June 27.[93]

Questions have been raised about the way Directions were formulated on the grounds of no open consultation to take into account feedback from all stakeholders – the public, civil society, cybersecurity experts, privacy advocates, and the private sector. Multiple Virtual Private Network service providers have decided to shut down their servers in India. Both ExpressVPN and Surfshark have shut down their servers in response to the CERT-In directions.[94]

Nord, Proton, Express, Surfshark, Windscribe, and Mullvad, popular VPN service providers, objected to the new rules while making it clear that they will not comply with the new directions because of a lack of technical feasibility. Industry bodies raised their concerns against the directive arguing that it will make doing digital business in India tougher. In a letter they stated, "detrimental impact on cybersecurity for organisations that operate in India, and create a disjointed approach to cybersecurity across jurisdictions, undermining the security posture of India and its allies in the QUAD countries, Europe, and beyond".[95]

Recommendations

From the above analysis, it is clear that restrictions on cross-border data flow can make doing business difficult for digital businesses, especially smaller ones, at a significant level. In this context, to provide for EoDDB while also addressing legitimate concerns, a few recommendations are highlighted below:

1. Encouraging Transparency

Data protection mandates should take a balanced approach between safeguarding the privacy of individuals, and sovereignty and promoting a receptive environment for doing digital business. Recognising legitimate concerns would be critical in building trust and optimal data governance frameworks.

In this context, instead of bringing hard data localisation norms, the Indian government should encourage firms to improve consumer trust through greater transparency about how they manage data and support the development of global data-related standards. This can be done by adopting principles such as data minimisation, retention and minimising third-party access with appropriate safeguards.

Firms should also ensure transparency for consumers by using different models such as dynamic consent[96] and easy-to-use proxy[97] systems that give more control to consumers over their data.

To ensure data remains secure, organisations should have appropriate technological, organisational, and physical safeguards in place. In the current scenario, data localisation norms override individual preferences, rather than seeking to enable individuals to make more informed decisions by equipping people with better data literacy skills and encouraging more transparency in the data processing. In addition, regulators need to define the objectives of the policies and process to achieve the same more clearly and periodically analyse their impact before taking any decisions. By seeking inputs from relevant stakeholders such as Law Enforcement Agency (LEA), and consumer protection organisations, digital business firms can help to ensure a fair assessment between cost and benefits.

2. Harmonising with International Norms

As the above-discussed issues stem from new-age globalisation enabled by digitally-mediated architecture, the solution should also be sought from global cooperation by strengthening data governance models. At the G20, India can pursue countries for global cooperation for data sharing to realise more equitable global economic growth.

To this end, India should be advocating the need for establishing trust among stakeholders including developing countries, regulators, consumers, industry and LEA and should underscore implications of legal certainty for the growth of doing digital business. A coordinated dialogue about how to safeguard privacy and security, while reaping the economic and societal benefits of sharing data within and across borders, will lead to less intrusive models of data regulations.

By going beyond the current design of the Osaka Track, India should bring discussion and its perspectives to global forums that will build a shared understanding around standards, costs, and the

solutions available to address ideological, privacy, security and technical concerns. This will create the paths for adopting greater standards of rights-protective data protection principles and frameworks.

3. Strengthen Cross-Border Data Flows

There is a need for developing a progressive global architecture for data flows. While protecting its interests, India should actively participate in global efforts of ensuring cross-border data flow. Some multilateral efforts are taking shape globally to make compliance more manageable for digital businesses, and to reap the benefits of cross-border data flows.

For example, through Digital Economy Agreements (DEAs), Singapore, Australia and the UK attempt to address some of the risks and costs of a highly fragmented regulatory environment. Similarly, through the Digital Economy Partnership Agreement (DEPA), Australia, Chile, New Zealand, and Singapore are attempting to negotiate competing interests to ensure data flow among them. Such negotiation will not only strengthen the foundation for doing digital business but also consumers will benefit from an overarching set of global principles around a common understanding of how to regulate cross-border data flow.

India has also signed an agreement with the United Arab Emirates for cross-border data flow and agreed to negotiate with Australia on the same issue.[98] These processes need to be fast-tracked to ensure India does not harm its digital economic growth. Similarly, apart from the Trade Policy Forum and ICT working group, India should initiate dialogue with the USA on cross-border data flow by involving government officials, LEA, and trade agencies to achieve tangible objectives such as providing a conducive environment for doing digital business in both countries, addressing security concerns and providing definitional clarity. This will be important as the USA is a major exporting country of the Indian data-driven service sector.

4. Enhancing Data Security

The government may consider improving existing and building new mechanisms to enhance cross-border requests for data related to law enforcement investigations to provide timely assistance. Clarifying the Lawful Overseas Use of Data (CLOUD) Act and Mutual Legal Assistance Treaties (MLATs) have been erratic. Indian parliamentary committee report revealed that in 2021, India had 845 requests pending with various countries under these two processes.[99]

Drawing upon the Parliamentary Committee on External Affairs,[100] India should aim for building capacities such as training programs, standardisation of requests, and resource and time commitments for the handling of data access requests from abroad to effectively utilise such mechanisms. Further, India should also negotiate with its major digital trade partners including the UK, USA and Australia for better and more effective handling of undue delays and rejected requests.

Endnotes

1 Cory, Nigel and Dascoli, Luke, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', 19 July 2021, ITIF, available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

2 Taylor, D., Richard, 20 September 2020, '"Data localization": The internet in the balance', Telecommunications Policy, *available at* https://www.sciencedirect.com/science/article/abs/pii/S0308596120300951

3 Report of the JPC on the Personal Data Protection Bill, 2019, 2021, Ministry of Electronics and Information Technology, *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

4 Report by the Committee of Experts on Non-Personal Data Governance Framework, 2020, Ministry of Electronics and Information Technology, *available at* https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

5 Supra Note 3

6 *Ibid*

7 Ease of Doing Digital Business, 2022, CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER), available at https://cuts-ccier.org/eoddbj/; Discussion Paper on Impact of Criminalising Provisions on Ease of Doing Digital Business in India, *available at* https://cuts-ccier.org/pdf/dp-impact-of-criminalising-provisions-on-ease-of-doing-digital-business-in-india.pdf; Discussion Paper on Impact of Regulatory Uncertainty on Ease of Doing Digital Business, *available at* https://cuts-ccier.org/pdf/dp-impact_of_regulatory_uncertainty_on_ease_of_doing_digital_business.pdf; Discussion Paper on Impact of Inadequate Digital Infrastructure on Ease of Doing Digital Business in India, *available at* https://cuts-ccier.org/pdf/discussion-paper-on_impact_of_inadequate_digital_infrastructure_on_ease_of_doing_digital_business_in_india.pdf; Discussion Paper on Impact of Unnecessary Compliances Ease of Doing Digital Business in India, *available at* https://cuts-ccier.org/pdf/dp-on-impact-of-unnecessary-compliances-ease-of-doing-digital-business-in-india.pdf

8. Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow', 2021, United Nation Conference on Trade and Development, *Available at* https://unctad.org/system/files/official-document/der2021_en.pdf

9 Ibid

10 *Ibid*

11 *Ibid*

12 Chander, A., & Schwartz, P, 2022, 'Privacy and/or Trade', *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

13 Supra Note 1

14 *Ibid*

15 Supra note 1

16 Triplett, E. Jack, Bosworth, Barry, Productivity Measurement Issues in Services Industries: Baumol's Disease Has Been Cured, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=789545

17 Chander, A., & Lê, U, P. (2015). Data Nationalism. *64 Emory L. J.* 677 (2015). Retrieved from https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

18 Supra Note 12

19 Burman, Anirudh, 14 April 2021, 'How Would Data Localization Benefit India?', Carnegie India, *available at* https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

20' Supra Note 8

21 Cross-border data flows: Designing a global architecture for growth and innovation, *available at* https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation#:~:text=Cross%2Dborder%20data%20flows%20enable%20knowledge%20and%20data%20sharing%20and%20mitigation%20and%20adaptation

[22'] Supra Note 8

[23] Supra Note 12

[24] Localization of data privacy regulations creates competitive opportunities, *available at* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities

[25] Beyond Personal Data: The Cost Of Data Flow Restrictions To EU Companies, *available at* https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf

[26] Washington Post, 07 May 2019, 'The Technology 202: Activists Turn to Facebook Shareholders in Long-Shot Bid to Oust Zuckerberg,' *available at*, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/05/07/the-technology-202-activists-turn-to-facebook-shareholders-in-long-shot-bid-to-oust-zuckerberg/5cd10b1b1ad2e506550b2f81

[27] *Ibid*

[28] The Data Localization Debate in International Trade Law, *available at* https://www.ikigailaw.com/the-data-localization-debate-in-international-trade-law/#_ftn10

[29] Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, *available at* https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

[30] Collective action can spark innovation for data flows, *available at* https://www.chathamhouse.org/2021/06/collective-action-can-spark-innovation-data-flows

[31] G-20 Osaka summit: India refuses to sign declaration on free flow of data across borders, *available at* https://indianexpress.com/article/india/g-20-osaka-summit-narendra-mod-india-declaration-on-free-flow-of-data-across-borders-shinzo-abe-5805846/

[32] Supra Note 3

[33] *Ibid*

[34] *Ibid*

[35] Sensitive personal data includes information which may reveal, be related to, or constitute — financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation.

[36] Supra Note 3

[37] *Ibid*

[38] *Ibid*

[39] *Ibid*

[40] *Ibid*

[41] Basu, Arindrajit., Hickok, Elonnai., & Chawla, Singh, Aditya, Singh, 19 March 2019, 'The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India' *available at* https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

[42] Supra Note 19

[43] *Ibid*

[44] Quantifying the Cost of Forced Localization, *available at* https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localization

[45] Cloudy with a chance of data centres, *available at* https://the-ken.com/story/cloudy-with-a-chance-of-data-centres/

[46] No Data Beyond This Point! – Reducing the Risk of Cross-Border Data Transfers Through Effective Information and Data Governance, *available at* https://www.connectontech.com/no-data-beyond-this-point-reducing-the-risk-of-cross-border-data-transfers-through-effective-information-and-data-governance/

[47] How India faces Unique Data Centre Infra Challenges, *available at* https://w.media/how-india-faces-unique-data-centre-infra-challenges/

[48] Data Localisation India's Double-Edged Sword?, *available at,* https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf

[49] Kumar, B., & Rakheja, H, 2022, 'Will the Indian IT industry sustain its growth momentum?' *available at* https://www.business-standard.com/podcast/technology/will-indian-it-industry-sustain-its-growth-momentum-122012800079_1.html

[50] Supra Note 21

[51] CUTS International, 'Digital Trade and Data Localization', *available at* https://cuts-ccier.org/pdf/project-brief-dtdl.pdf

[52] Bauer et al, Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation, Paper Series: No. 30, Global Commission on Internet Governance, available at https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization/#:~:text=This%20methodology%20allows%20for%20the,relatively%20intensively%20on%20data%20services

[53] Supra Note 51

[54] Trading in US-India Data Flows Prospects for Cooperation in US-India Data Policy, *available at*, https://www.atlanticcouncil.org/wp-content/uploads/2022/03/Cross_Border_Data_Flows.pdf

[55] Supra Note 25

[56] The economic costs of restricting the cross-border flow of data, *available at*, https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625036783000

[57] Supra Note 56

[58] *Ibid*

[59] *Ibid*

[60] Cory, N., Luke, D. (2021). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Retrieved from https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

[61] Supra Note 17

[62] RBI Notification on Storage of Payment System Data 2018, *available at* https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

[63] Bhatia, Kalindhi, 25 September 2021, 'India: RBI's 2021 Ban On Amex And Diner's Club', *available at* https://www.mondaq.com/india/financial-services/1114668/rbi39s-2021-ban-on-amex-and-diner39s-club

[64] Supra Note 62

[65] *Ibid*

[66] Live Mint, 23 March 2022, India made 7442 cr digital payments FY22 at 33% growth rate: MeitY, *available at* https://www.livemint.com/technology/tech-news/india-made-7-422-cr-digital-payments-in-fy22-at-33-growth-rate-meity-11648038672792.html

[67] Supra Note 62

[68] Mehrotra, Karishma, 19 October 2019, Data localisation: why, why not, Indian Express, *available at* https://indianexpress.com/article/explained/data-localisation-rbi-guidelines-banking-why-why-not-5408177/

[69'] Data Divide', 16 April 2022, Business Line, *available at* https://www.thehindubusinessline.com/opinion/editorial/india-should-continue-its-efforts-to-localise-data-notwithstanding-ustrs-protestations/article65324189.ece

[70] Data localisation in India: Significance and economic impact, *available at*, https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-localisation-in-india-significance-and-economic-impact/85292096

[71] Singh, Pal, Ashok, PAL, 30 July 2021, 'RBI's Mastercard Ban: Overkill, With A Touch of Protectionism', The Quint, *available at* https://www.thequint.com/voices/opinion/rbis-mastercard-ban-regulatory-overkill-with-a-touch-of-anti-americanism#read-more#read-more

[72] Live Mint, 14 December, 2019, Google wants US Federal Reserve to follow India's UPI example and build 'FedNow', available at https://www.livemint.com/news/india/google-wants-us-federal-reserve-to-follow-india-s-upi-example-and-build-fednow-11576335813947.html

[73] IRSG Report – How the trend towards data localisation is impacting the financial services sector, *available at*, https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/

[74] Data localisation may hinder credit card fraud detection: Mastercard, *available at*, https://www.expresscomputer.in/security/data-localisation-may-hinder-credit-card-fraud-detection-mastercard/34099/

[75] The Great India Data localization puzzle , *available at*. https://cio.economictimes.indiatimes.com/news/big-data/the-great-india-data-localization-puzzle/89787780

[76] Supra Note 73

[77] Supra Note 73

[78] *Ibid*

[79'] RBI restricts American Express, Diners Club from on-boarding new customers from May 1', 23 April 2021, The Hindu, *available at* RBI restricts American Express, Diners Club from on-boarding new customers from May 1 - The Hindu

[80] Supra Note 73

[81] Verma,Mimansa, 20 May 2020, 'Apple has halted card payments for its in-app subscriptions in India', Quartz India, *available at* Apple has halted card payments for its in-app subscriptions in India

[82] Explained: How RBI's restriction on Mastercard impacts banking network, existing customers', 15 July 2021, India Today, *available at* Explained: How RBI's restriction on Mastercard impacts banking network, existing customers - Business News

[83] Nair, Vishwanath, 'RBI Lifts Restrictions On Mastercard In India', 16 June 2022, Bloomberg Quint Prime, *available at* RBI Lifts Restrictions On Mastercard In India

[84] RBI lifts restrictions on Mastercard over onboarding new customers, June 17, 2022, *available at* https://www.business-standard.com/article/finance/rbi-lifts-restrictions-related-to-on-boarding-new-customers-on-mastercard-122061600884_1.html

[85] Parkin, B, How US payments groups ended up on the wrong side of India's plans, 21 August 2021, Financial Times, *available at* How US payments groups ended up on the wrong side of India's plans

[86] *Ibid*

[87] 28 April 2022, 'Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet,' Ministry of Electronics and Information Technology and Indian Computer Emergency Response Team (CERT-In), *available at* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[88] IBM News Room, 'IBM Report: Cost of a Data Breach Hits Record High During Pandemic', IBM, *available at* https://in.newsroom.ibm.com/IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic?lnk=hm

[89] *Ibid*

9 Chapter Digital Stories from the Ground

Introduction

The Government of India (GoI) has put a special focus on the Ease of Doing Business in India. There have been multiple reforms in regulations and policy decisions, which have led to advancement of the Indian economy. Similar advancements are desired for digital business and to facilitate their Ease of Doing Digital Business (EoDDB).

This study undertook comprehensive secondary research on various identified issues and challenges faced by digital businesses in doing business, which have been covered in previous chapters of this report. To further understand the nuances of these issues, interaction with relevant stakeholders including digital businesses was warranted.

Interaction with key stakeholders helped in filling the gaps in publicly available information and provided a deeper understanding of the implications of policies, regulations and infrastructure in doing digital business in India. These interactions were carried out in two phases. At first, digital businesses were interviewed to gauge their perspective. For this purpose, semi-structured interviews were conducted with a total of 15 digital businesses from different sectors (ecommerce, gaming, fin-tech, social media) operating in India, through various means including in-person and telephone interviews.

The in-person and telephonic interviews allowed researchers to delve deep into individual experiences of digital businesses and the persons who manage the impact of regulations on digital businesses. The exercise brought forth on-ground realities for digital businesses, which has made this report robust and credible. These experiences have made this research focussed on solutions, which will resolve challenges faced on ground by digital businesses including businesses in their nascent stage.

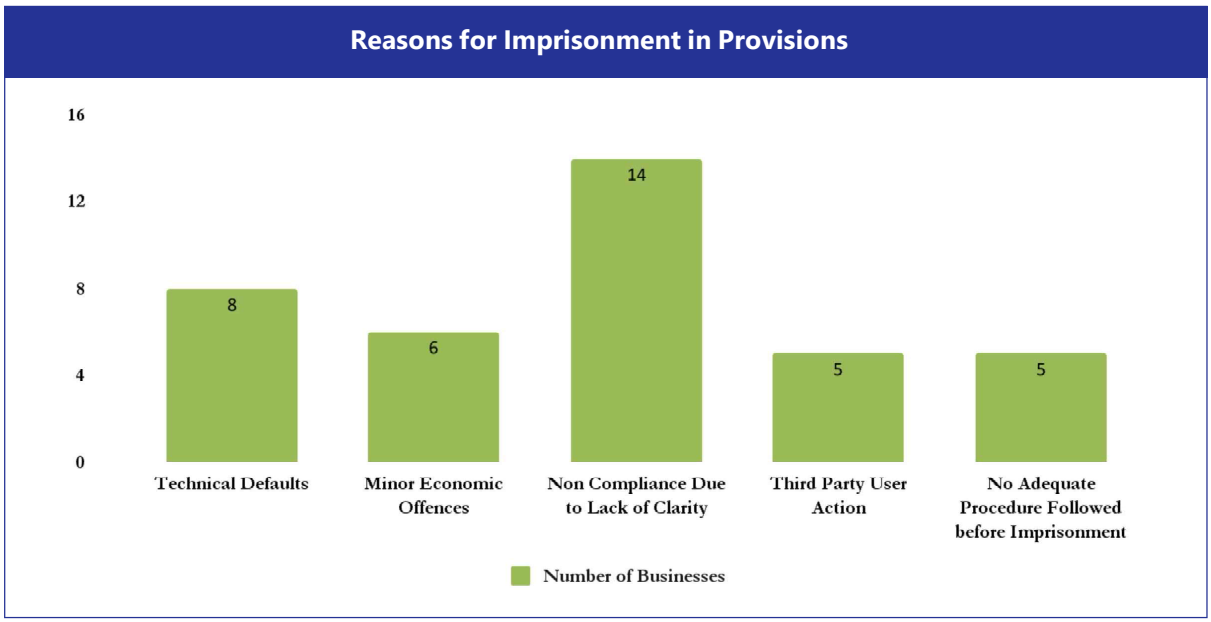
A major challenge during this process was gaining access to the people working in the policy vertical of the digital business ecosystem. In light of this limitation, the researchers have protected the anonymity of the interviewees and the digital businesses.

Later on, a focus group discussion (FGD) with experts, including representatives from government, think tanks, industry, law and consulting firms, and digital businesses was conducted to gain further insights. Their feedback and suggestions were sought on ways to meet valid regulatory objectives without unnecessarily impacting EoDDB.[1]

Interaction with Digital Businesses

A. Imprisonment/Criminalising Provisions

Out of 15 digital businesses, seven find imprisonment provisions as one of the most important factors impacting EoDDB. It is important to know that businesses who function in the domain of E-commerce, Ed-tech, Online Freelance and Online Gaming are most concerned about the provisions of



imprisonment. The reasons for provisions to prescribe imprisonment can be summarised into technical defaults, minor economic offences, non-compliance due to lack of clarity, third party user action and non-adequate procedure followed before imprisonment (such as no-show cause notices, review of requests).

One of the reasons that employees of businesses face the fear of imprisonment is because of non-compliance with the requirements of the law or executive direction or order. However, often the laws and executive orders are not very clear on the actions that a business might have to undertake, considering which, unnecessary delays leading to non-compliance happen. As many as 14 businesses considered 'non-compliance on part of businesses due to lack of clarity in provisions and process' as a reason for imprisonment as most problematic, while few considered 'minor economic offences' such as those under Section 26 (1) and 26 (4) of the Payment and Settlement System Act, 2007 (PSSA) and other 39 minor offences that the Ministry of Finance had recognised for decriminalisation[2], as a reason for imprisonment to be problematic. We found that start-ups and nascent stage digital businesses remain unaware of such imprisonment provisions and their potential impact on their businesses.

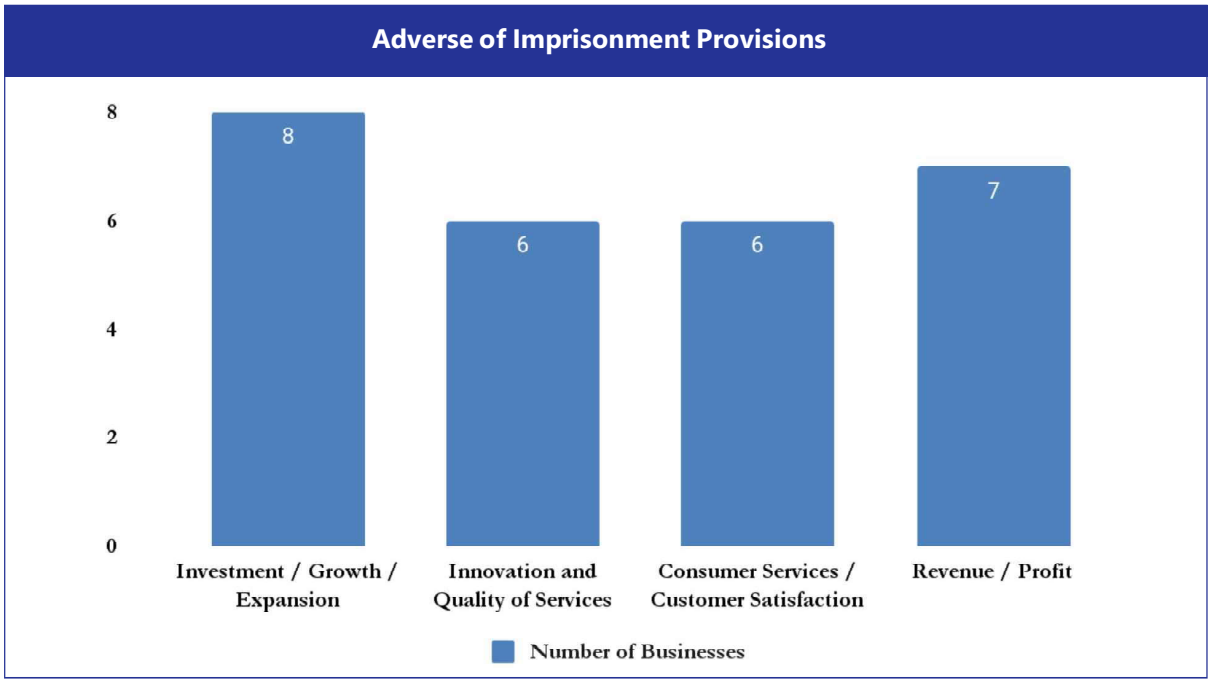
As highlighted in our chapter on impact of criminalising provisions on EoDDB,[3] all major regulations and laws pertaining to digital business contain provisions for imprisonment, largely placing the burden of compliance on bigger businesses. These provide small businesses with affordable, scalable, and secure business solutions.[4] If any of these businesses decide to leave India due to over-regulations and criminalisation; there will be a definite impact on thousands of small businesses that use these platforms.

Over half of the businesses that were consulted considered that imprisonment for non-compliance due to technical defaults is problematic in nature. We found through secondary research that technical provisions often carry disproportionately large penalties in the form of imprisonment. The government had previously sought to decriminalise over 110 archaic provisions constituting economic offences,[5] however, this has not materialised. Similar economic offences have been observed in the PSSA, where Section 26(1) even after being technical and procedural as determined by the Ministry of Finance, prescribes imprisonment ranging from as little as one month to as extreme as 10 years or fines or both.

From our contacted businesses, only five placed importance on imprisonment due to 'third party user action' such as 'employees being jailed for platform/business hosting the content uploaded, created etc. by users' being problematic for digital businesses. However, in our secondary research we found that one of the key reasons for actions taken in India and abroad against digital businesses are due to third party user actions. However, in countries other than India, there are effective liability shields or safe harbour provisions in place, which protect businesses from such user action.

Further, five businesses regarded 'no adequate procedure followed before imprisonment' such as 'lack of notice and show-cause processes' as problematic. Our findings through secondary research highlighted that most imprisonment provisions do not have any procedural safeguards or if safeguards are present they remain practically unused before an employee is imprisoned. For instance, Section 69A of IT Act and blocking rules under the same have procedural safeguards, which remain unused. Our findings support the findings from secondary research.

Furthermore, we also asked how imprisonment provisions adversely impact businesses and the response is summarised in the following graph.



We placed our findings from secondary research and stakeholder interactions before a group of experts. This was done to seek a way forward for dealing with the impact of imprisonment provisions on businesses. Following is a brief summary of our interaction:

In economic theory, trust and economic development go hand in hand. Economies that have better trust develop faster. Resolving the problem of trust deficit is a structural and process issue as it cuts across different sectors and legislation. It's important to flip the narrative where the default should be to trust business entities. If something adverse happens, regulation should be brought in.

There are several examples of criminal liability and compliances making it difficult for businesses to hire. For instance, IT Rules, even smaller businesses are being burdened with regulations that should come in only for Significant Social Media Intermediaries (SSMIs). In practice, having a criminal liability framework works seldom because fundamentally and philosophically, it creates an atmosphere of distrust where everybody is suspicious of each other. The government is suspicious of business and the business is suspicious of the government. Business does not trust that the government will think that they are there with good intentions and good faith and vice versa.

Further, criminalising provisions keep the person responsible on the hook for making sure that the rules are compiled with. Because policies create criminal and personal liabilities on founders and staff that have to be employed for compliance like the grievance officer, it only adds up to an atmosphere of psychological pressure, which prevents business owners from doing business but makes them focus on how to do a particular compliance.

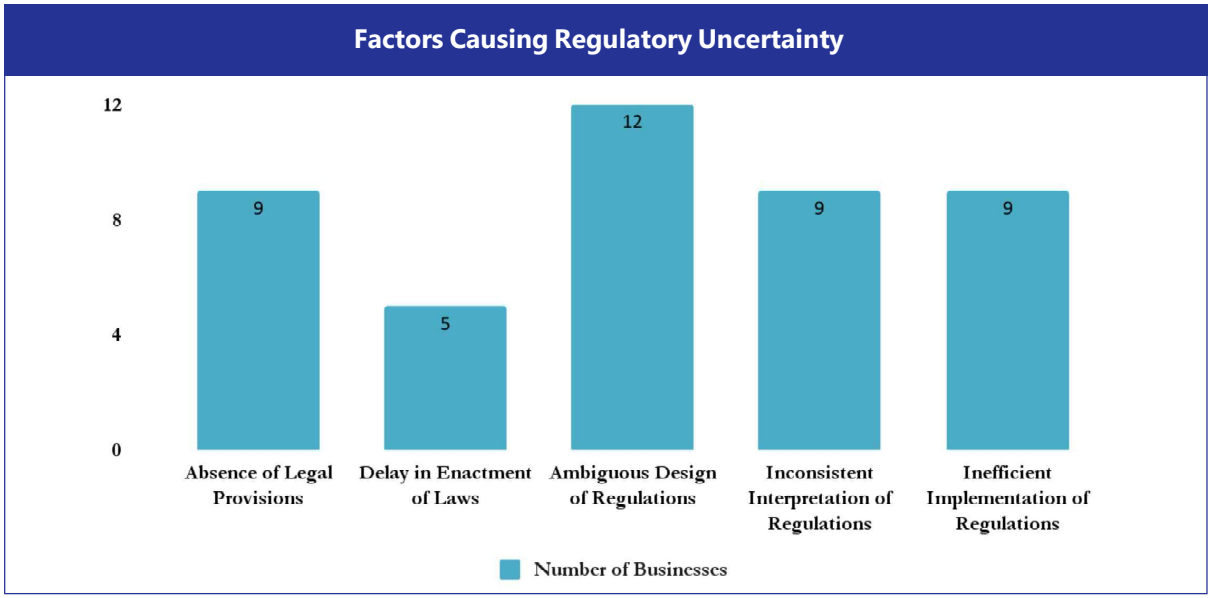
Furthermore, law enforcement agencies (LEAs) often get involved to curb cyber crimes. For instance, there are cases where digital businesses running financial services are held up by the Enforcement Directorate (ED) for frauds happening using their platforms. The digital business may not be aware of such happenings or who is doing it. There is no clarity on what kind of information the digital business is expected to give.

The government may have the right intent but building trust in the ecosystem is required to create transparency about the objectives of the regulator. Thus, there is a need to explore frameworks, which go beyond criminal and personal liability. For building trust, the government needs to look at other avenues like Pre-Legislative Consultation Process (PLCP), Regulatory Impact Assessments (RIA) and Cost-Benefit Analysis (CBAs), which are small starting steps to help build that trust.

B. Regulatory Uncertainty

Most businesses are highly affected by regulatory uncertainty. Out of the 15 digital businesses, 10 gave regulatory uncertainty high importance in terms of impacting EoDDB. As highlighted in the chapter on impact of regulatory uncertainty on EoDDB, regulatory uncertainty can be caused because of various reasons. These include lack of legal and regulatory frameworks, delay in the enactment of proposed laws, arbitrary approach of issuing regulations, sub-optimal or ambiguous design of regulatory framework and inconsistent interpretation of the regulatory instrument. The following graph summarises what businesses consider factors when looking at regulatory uncertainty.

When asked about the aspects, which cause regulatory uncertainty, 12 out of 15 businesses stated that ambiguous design of regulations causes regulatory uncertainty. However, delay in enactment of new laws may not be a big concerning factor contributing to regulatory uncertainty as 10 out of the 15 digital businesses considered it not to be a factor.



Road to Becoming the World Leader of Web 3.0 is Obstructed with Regulatory Uncertainty

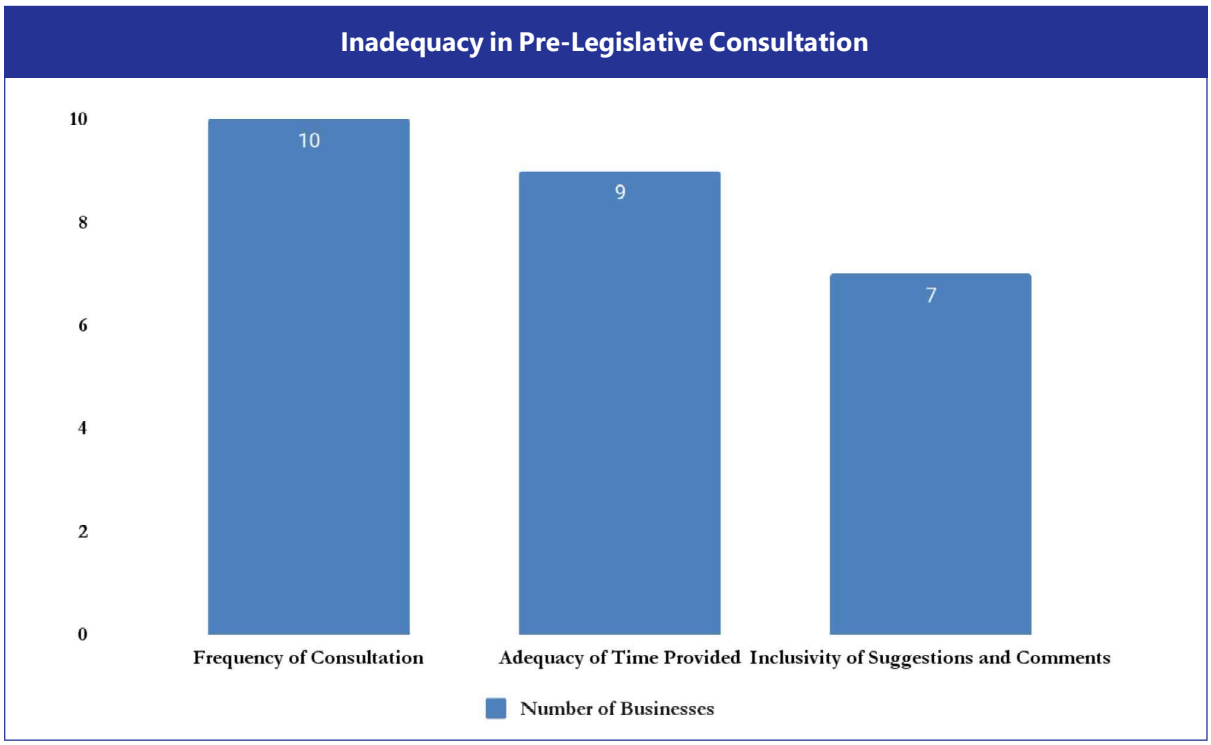
An e-commerce start-up stated that it was keen on foraying into the world of Web3.0 and wanted to explore opportunities in the blockchain, crypto and metaverse space. The start-up also had the required capacity and massive funding opportunities. However, due to the looming regulatory uncertainty in this space, it was unwilling to venture into Web3.0. Highlighting the recent changes in cryptocurrency regulation like taxation on crypto assets, the start-up further stated that there were frequent and arbitrary changes, which were making digital businesses move to tax havens such as Cayman Islands and Dubai. The start-up suggested that a complete ban on crypto was not possible and the government is trying to dissuade investors by changing its stance every two-three months. Thus, lack of legal and regulatory framework coupled with arbitrary approach of regulation put barriers for digital businesses to venture into the space. Studies suggest that India has the tech, talent and startups to lead in the Web3.0.[6] However, due to the persistent regulatory uncertainty, this talent is moving abroad, which is a critical cause of concern for the Digital India dream.[7]

On the other hand, a few specific types of digital businesses found government laws and policies helpful in guiding their business decisions. For instance, ed-tech start-ups seemed to be fairly aware about government policies and regulations and mentioned that awareness helps them navigate their business decisions. A young ed-tech start-up was well aware about the regulatory issues that might crop up with the enactment of a data protection law because of its collecting data. The business had asked for their outsourced legal team to come up with a plan for the data protection bill and ed-tech regulations along with vision of digital education in the National Education Policy 2020. However, with how things have progressed in terms of data protection, the business stated that there is an uncertainty for their future steps for when such laws come in place. Another ed-tech start-up stated that the New Education Policy and the ed-tech regulations have impacted their businesses decisions. For understanding how sector specific regulations such as those in the ed-tech field impact businesses, please refer to the chapter on regulatory uncertainty.

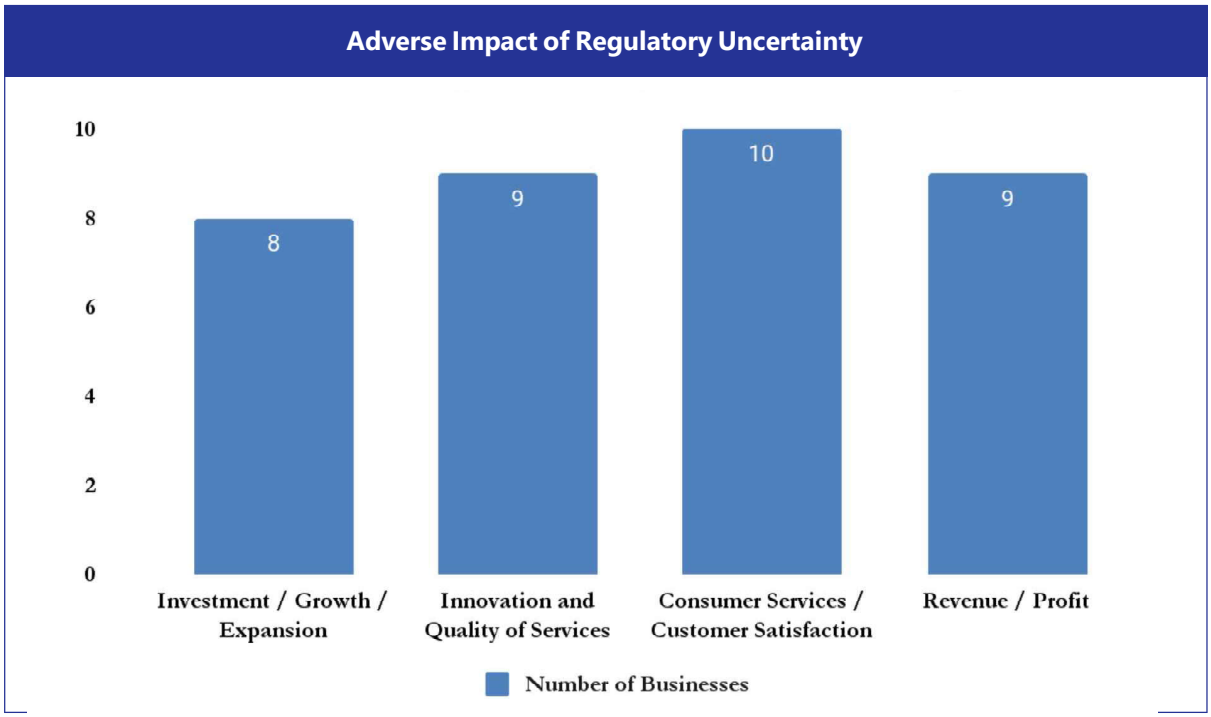
What do Businesses think about the Pre-Legislative Consultation?

For curbing regulatory uncertainty, following the Pre-Legislative Consultation Policy (PLCP) can help. As per PLCP, 2014 of the government, a minimum of 30 days should be provided to the public for making comments. As many as 12 out of the 15 interviewed businesses were aware that the government often carries out PLCP for major laws, policies and regulations. However, businesses seem to be dissatisfied with the overall process. Detailed findings are highlighted below.

Out of the 12 aware about PLCP, eight digital businesses stated that the frequency of consultation by the government was inadequate. Further, eight digital businesses stated that the time provided for making comments was inadequate. Furthermore, seven businesses also stated that the inclusion of suggestions given to the government was not made. It is indicative of the problem that the government, in spite of inviting comments, was not adequately addressing the concerns or being inclusive of diverse views. A few digital businesses stated that lack of consultation, unpredictable provisions and timelines to make comments also cause regulatory uncertainty. It has to be noted that, at several instances, the government has skipped the process or has not provided adequate time for the public to make comments. The matter has also been previously raised in the Parliament by the opposition.[8]



With respect to regulatory uncertainty impacting specific parameters of EoDDB, it was observed that investments are impacted for e-commerce, gaming and digital financial services businesses. Further, for e-commerce firms, regulatory uncertainty also impacts innovation, consumer satisfaction and revenue and profits. Similarly, regulatory uncertainty also negatively impacts digital media video streaming businesses with respect to innovation, consumer satisfaction and revenue and profits. A total of eight digital businesses stated that regulatory uncertainty impacts consumer satisfaction. Thus, as discussed in the chapter on impact of regulatory uncertainty on EoDDB, regulatory uncertainty can hugely impact businesses and they may pull out their investments, ultimately affecting the digital economy.



The findings from secondary research and interactions with stakeholders were placed before a group of experts. This helped in seeking a way forward for dealing with the impact of regulatory uncertainty on businesses. Following is a brief summary of our interaction:

Digital policies in India have to be better articulated. Stating broad objectives like digital growth of India is not enough because the same could be achieved through multiple ways. Thus, what has to be achieved and the pathways to achieve it need to be figured out. Further, many regulators try to achieve similar goals and here, many issues go unaddressed. Regulators have to align on common objectives and adopting a common regulatory framework will help. There may be a need to assess different regulatory frameworks to arrive at the most conducive one. Such different regulatory frameworks include models of self-regulation, co-regulation, creating regulatory sandboxes and forming inter-ministerial groups, among others. A vision document for the digital ecosystem similar to what the United Kingdom (UK) or other countries may be created. It will act as a starting point for all regulators to chart out what they seek to achieve in detail. Further, there is a need to examine the sources of friction by juxtaposing regulatory framework for traditional businesses with regulatory framework for digital businesses.

Further, there exists dissonance between narratives and ground realities and it is difficult to analyse regulatory perspectives. For having optimal regulation, regulators must conduct themselves transparently and should start with good faith. However, many times, digital businesses get to know about a regulator's intentions or actions through leaked media reports. Opacity in the regulatory and policy development process as well as the extended timelines cause regulatory uncertainty. For instance, law for data protection has been in the making for more than five years, which has caused anxiety for digital businesses.

Further, there should be open communication about issues being faced by the industry. Solutions should be arrived at with a consultative stakeholder engagement to help reduce information asymmetry and find out the problems implementation of policies may bring in. Many times, instead of a genuine participatory approach, there is a reactionary approach taken by governments, to please the general narrative of the media. Unless there is a two-way conversation between the regulator and the industry on issues and challenges faced by each of them, an effective solution cannot be reached. Instituting mechanisms where industry stakeholders' conversations are planned and become transparent as opposed to sporadic and reactionary, is needed. Designing a continuous consultative regulatory framework is necessary because as technologies evolve, newer challenges will come up. Studies have shown that collaborative policy processes where stakeholders are asked for their perception of specific policies before reform are likely to be more satisfied with the new policies.[9]

Herein, feedback loops are important. There needs to be a responsive regulation pyramid. It needs to happen at three levels: (i) at the time of defining the problem statement by deploying market monitoring tools to see what the problem areas are; (ii) at the time of coming up with solutions by doing consultation with all stakeholders, which is a model of co-regulation; and (iii) at the time when regulation is in place to check how the market is responding to them.

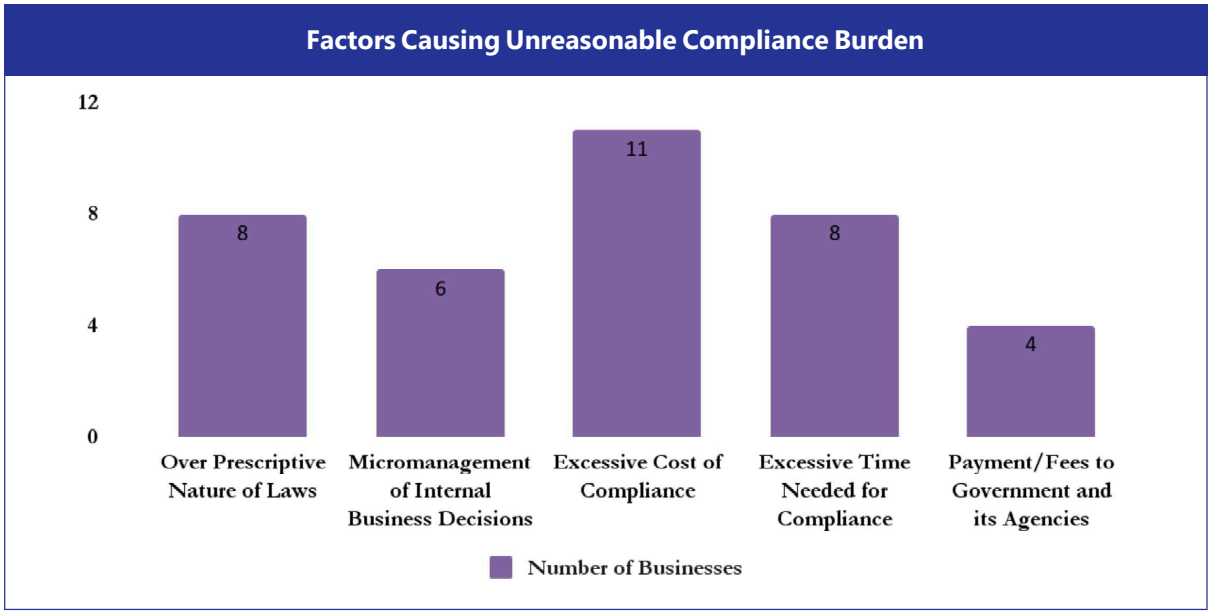
In order to design solutions, constant market monitoring such as utilising regulatory technology (regtech) and analytics can be helpful toolkits for regulators. The idea is to gauge sentiment of the market, on the consumer and business sides in real time. This can be used as evidence to inform policy decisions. Currently, even when regulators utilise such mechanisms, it is not transparent and thus, an outsider is sceptical. Utilising these different regulatory tools in a transparent manner could help bridge a trust deficit as well.

Often, the role of government, both central and state, has been very detrimental in deciding how businesses face compliances and how businesses will function. In the digital ecosystem, central governments can enable a better regulatory landscape as compared to state governments. However, be it the central or the state governments, the principles and the objectives of regulation continue to apply and should be within the constitutional framework. There is a need to think whether the central government needs to play a more active role to bring everybody on the same page, to bring about regulatory certainty. Further, experts opined that a structure and framework, which works for all stakeholders needs to be drawn for sectors like online gaming where in both, centre and state governments can formulate policies. Whether the centre plays a more active role in regulation or lays

out model guidelines, which different states can adopt or a structure where different states come together to draw a common regulatory framework needs to be worked out.

C. Unnecessary Compliances

Unnecessary compliances in regulations are often the cause of discomfort for digital businesses. Out of the 15 digital businesses, over 12 businesses placed compliances and their burden as the most important parameter for EoDDB in India and none believed that it is not an important parameter for EoDDB in India.



In our previous chapter on "unnecessary compliances and their impact on EoDDB" we highlighted that though the burden of compliances is on all businesses, it is complex for smaller businesses and also places disproportionate costs on them.[10]

Out of 15 businesses, eighth placed 'excessive cost of compliance' as a leading cause of unreasonable compliance burdens for digital businesses, with 'over prescriptive nature of laws' running close behind with seven businesses placing this as a cause for unnecessary compliance burdens. Further, an Ed-Tech Start-up based in Jaipur, which connects students and teachers with the help of classroom technology is engaged with our team on the issue of EoDDB vis-a-vis the position of start-ups in India.

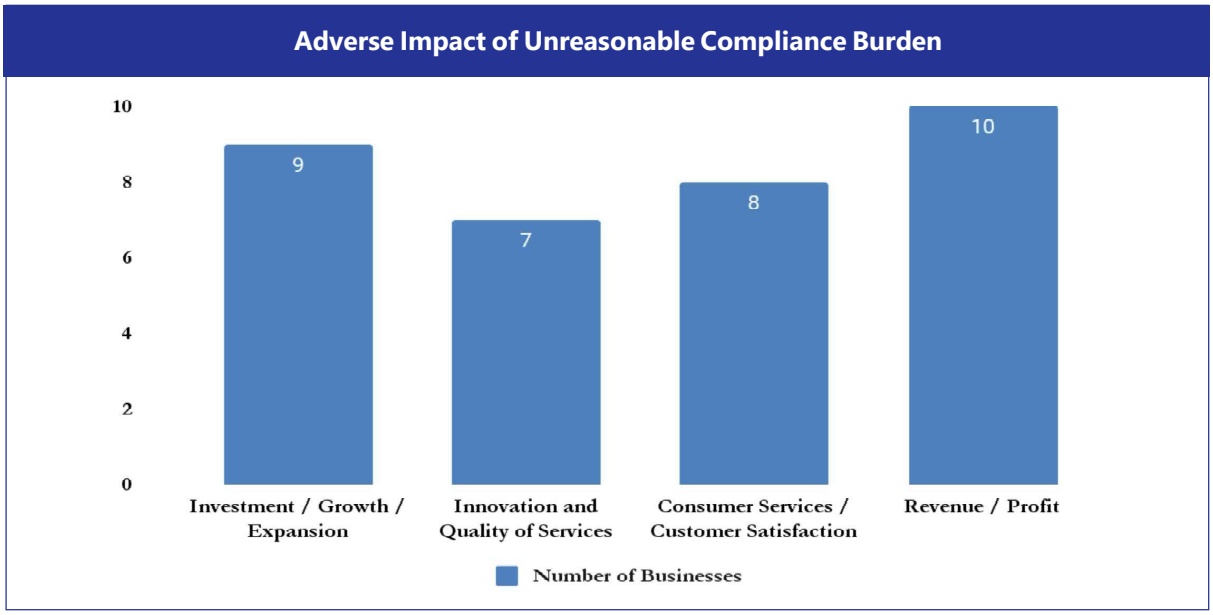
This business has outsourced their **compliance requirements** to their Chartered Accountancy (CA) firm, however, is unaware of the compliance mechanisms. The outsourced company only bills the businesses for their services.

However, the compliance requirements that the founders keep track are that of Goods and Services Tax (GST) filing and Income Tax returns of both the company and directors. It would be beneficial for tech-based businesses to have compliances, which are digitised and automated in nature. For instance, the Director of any business needs to file their Know Your Customer (KYC) requisites every financial year.[11] However, as the business has already provided for government-linked identity proofs like PAN Card, AADHAAR and bank details, these KYCs can be automated. The RBI has also launched a Central KYC Records Registry, to enable consumers open multiple account-based relationships through KYC identifiers, without unnecessary repeated submission and sharing of sensitive customer information. The Rules can enable intermediaries to utilise such KYC identifiers, for customer verification.[12] The previous chapter on compliance burden also found that, periodic and repetitive compliances are an additional burden on companies, which are not as resource laden as big tech and thus such compliances are discriminatory and unnecessary in nature.

Out of the 15, five regarded 'micromanagement of internal business decisions' as a reason for unreasonable compliance burden. We observed the same in our previous chapters in regards to the Intermediary Rules 2021. Under the rules, appointment of new officers for compliance and grievance were specific to their qualification and roles in the digital businesses and very specific liabilities were associated with these new roles. This led to scepticism in businesses about the liabilities attached to the role[13] while their freedom for businesses' internal decisions was taken away.

While only four and three businesses placed '*excessive time needed for compliance*' and '*payment/fees to government and its agencies*' respectively as important factors for increased unreasonable compliances. One unique finding from our interactions with start-ups was that the businesses are not aware of the compliance requirements and prefer to outsource the same to their CA firms. One e-commerce aggregator based in Jaipur claimed that, initially, most start-ups get to know about the legal requirements through peer-learning.

In our interactions with businesses, several businesses operating in the sphere of online gaming, online freelance, e-commerce, subscription based digital media noted that unreasonable compliances negatively impact their plans of investment, growth and expansion. From the same category of businesses, it was found that the negative impact also seeps into their prospects of innovation and hampers their quality of services. In our previous chapters we found that excessively prescriptive regulations also disincentivise businesses from innovation, often for marginalised consumers.



Most businesses remarked that the cost of compliances and their unreasonableness lead to negative impact on revenue, profit and businesses' initiative towards bettering consumer services. We found the same in our previous chapters, where RBI's recurring payment guidelines caused smaller businesses to lose out on high percentages of revenue, which was disproportionate to the losses of businesses with larger resources.

The findings from secondary research and interactions with stakeholders were placed before a group of experts. This helped in seeking a way forward for dealing with the impact of regulatory uncertainty on businesses. Following is a brief summary of our interaction:

Policies have a stated objective. There is little to no quarrel with such stated objectives. For instance, removal of harmful content that exists on social media platforms or the need for having a personal data protection bill are well recognised. However, the challenge is to identify whether the prescribed means achieve the objectives that have been laid out and establish greater accountability of digital businesses is contentious. There exists a tremendous amount of disconnect between the objectives of a policy and what implementation leads to.

There is very little consultation with the entities, which have to comply with the directions in these policies. For example, the new CERT-In directions impose infrastructure costs and cost of workforce to be deployed for ensuring compliance on digital businesses. A unidirectional nature of issuing directives, where digital businesses are not consulted enough and have to ultimately figure out how to comply with it. It is unsurprising that digital businesses are not ready to comply on the day when these policies are enforced.

Further, the cost of non-compliances is also huge and disproportionate. For example, non-compliance to the IT Rules 2021 framework risks firms losing out on safe harbour provisions. Herein, there is a need to explore if different kinds of frameworks like penalties or fines can be put in place instead of removing safe harbour provisions.

There are several ways, in which an unnecessary compliance burden may be reduced. Many times, policies and regulations are developed in isolation where stakeholders' views who will be responsible for implementing it are not being taken into consideration. There should be a middle ground in policy-making where a participatory approach involving all stakeholders should be followed.

Regulation is welcome wherever necessary. However, ex-ante impact assessment in the form of RIA is required for all regulations. RIA is one of the ways to determine whether regulations are serving the purpose they were designed for. The RIA will be incomplete until impact on consumers and other stakeholders are also taken into account. Therefore, RIA should not just look at immediate benefits from regulations but also at any spill over benefits. Further, while some stakeholders may be at a higher risk because of undesirable outcomes of regulations, others may not. Thus, RIA can help in adopting proportionate regulations for different stakeholders.

Further, defining desired outcomes in terms of numbers, as is the practice, may be useful. However, it is also critically important to define desired outcomes in qualitative and nuanced terms. This will help capture the experience of both businesses and consumers. For instance, a large proportion of people may be filing GST returns but their experience of doing it also needs to be taken into account.

Reducing compliances is one of the ways to support small businesses. The cost of compliance because of a one-size fits all approach towards regulations hurts small and medium scale enterprises (SMEs). While SMEs should not be exempted completely from compliances because they too engage in clandestine activities, a graded approach may be adopted.

It may also be useful to incentivise compliance, as opposed to penalising non-compliance. All laws that are created with good intentions are resulting in digital businesses doing compliance just for the sake of doing compliance. For instance, digital businesses are not concerned if actual privacy protection is there on the ground as they are more concerned about whether they will be fined or not and what is the least that can be done to prevent these fines.

Escalation on non-compliances should be gradual and proportionate. Setting up a rule-based mechanism of escalation by stating consequences of non-compliances such that these consequences remain consistent over a long period of time will ease the stakeholders. It will create trust for digital businesses as well as consumers. However, there is also a need to maintain caution against proportionate regulation. When regulatory capacity is limited, it may be important to use it judiciously. However, in the digital ecosystem, regulators also need to be watchful because smaller firms could throw up data protection and privacy risks, such as those of Cambridge Analytica, which was not a big firm but the

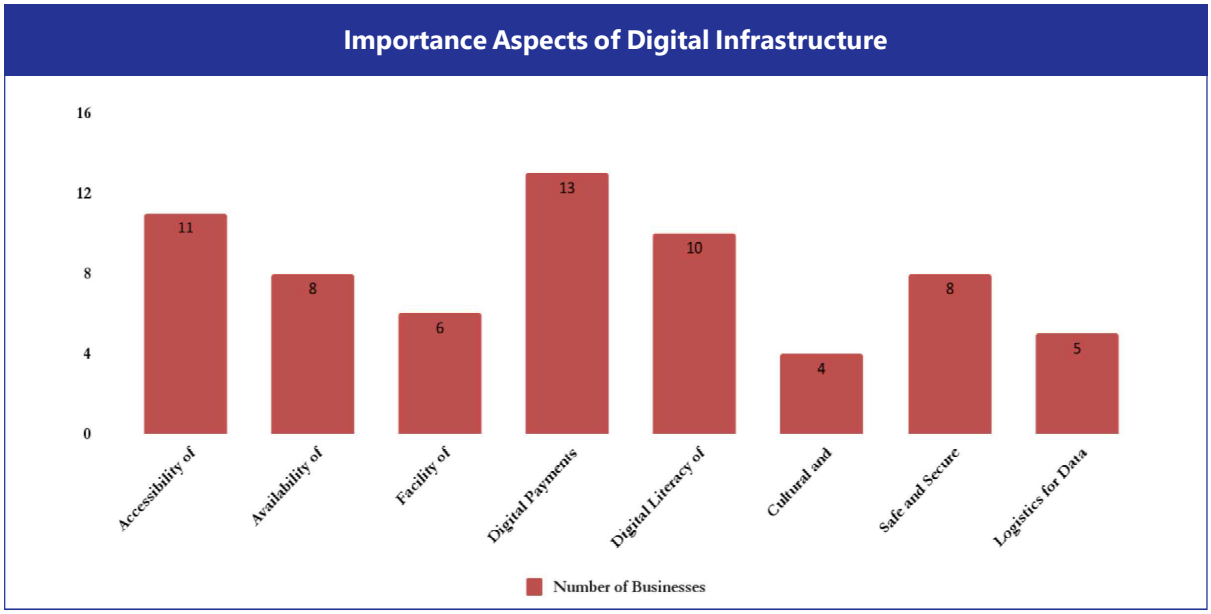
implications were severe. This could have been handled by use of technologies of regulation (reg-tech) and supervisory technologies (sup-tech) for close watch on entities and protecting consumers' privacy.[14]

There is also a need to understand the parameters that make an entity risky. The digital ecosystem works differently where smaller turnover businesses can inflict significant harm. Thus, these have to be different from the traditional parameters such as capital. The idea of proportionality is tethered to capital, turnover and profit but maybe there is a need to expand that so that the law of proportionality can then be applied in a more effective manner.

For example, digital lending has been spiralling out and lessons can be drawn from the financial sector. Non-Banking Financial Companies (NBFCs) had a smaller turnover and were not under the direct radar of the RBI. As NBFCs were smaller, the RBI practised proportionate regulation and utilised little regulatory capacity. However, many malpractices were done by NBFCs and inflicted extreme consumer harm.

D. Inadequate Digital Infrastructure

Most businesses with whom researchers have interacted stated that digital infrastructure is a critical factor in ease of doing digital business. Out 15, 12 digital business players say that digital infrastructure is highly important for them while only three of them say they view digital infrastructure as of average importance.



Further interaction informs the critical importance of the spectrum on digital infrastructure. For instance, 11 businesses said that high speed internet connectivity is important for their business. Six businesses said that infrastructure for facilitating Know-Your-Customers (KYC) is important for them. Ten businesses revealed that soft digital infrastructure such as digital literacy among consumers provides a comfortable environment for doing digital business.

The stakeholder engagement validates our findings of the chapter about inadequate digital infrastructure. The chapter establishes that lack of digital infrastructures has multiple direct and indirect impacts on doing digital business. Digital payment infrastructure is considered crucial by most businesses. As many as 13 out of 15 interviewed digital businesses, including both B2B and B2C businesses, considered having efficient digital payments infrastructure as critical for them.

Dispute Resolution

Know-Your-Customer (KYC), enabled by Aadhaar, has eased the identity verification but dispute resolution continues to be a challenge in doing digital businesses. It emerged as an important issue for digital businesses during stakeholder consultation. Thirteen out of 15 digital businesses stated that they found the time taken for dispute resolution cumbersome. Further, 12 digital businesses also found the cost of dispute resolution to be high. From a consumer standpoint, the process of dispute resolution is largely based on the chatbot, customer calling etc. which consumers find difficult to navigate. From a business standpoint, dispute resolution is not easy to navigate either. For instance, in an online financial transaction multiple parties such as banks and UPI platforms are involved, and it is not easy to find the error quickly. There is a need to ease grievance redressal mechanisms for both consumers and businesses.

Uninterrupted digital connectivity is also among top priority for digital businesses as digitally-mediated businesses have unmanageable dependencies on the digital connectivity. Growth of digital businesses demand online interactions, which are dependent on digital connectivity to use the business potential of digital businesses. Therefore, as interaction with digital businesses shows digital connectivity might not have direct impact but it has deep indirect impacts. In this regard, one of the start-ups, which operated in the e-commerce listing space stated that they are reluctant to expand their business in states where internet connectivity was impacted by internet shutdowns such as Jammu and Kashmir. The start-up was also reluctant to expand in states such as Madhya Pradesh and Chhattisgarh citing that they are Naxalite affected areas and it would cause difficulty in operations.

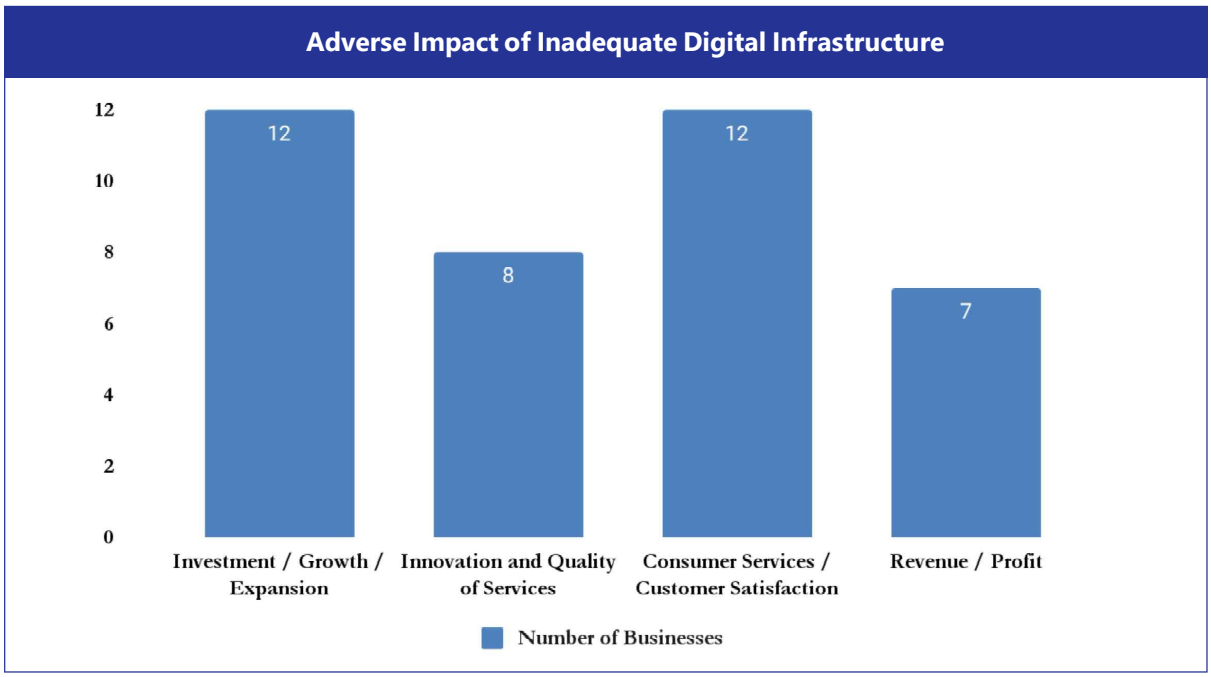
As the chapter highlights, internet shutdown has cost US$582 million in India, which is among top countries in shutting down the internet. Disproportionate internet shutdowns shake the confidence of business communities and allied stakeholders. Maintaining public order and national security has been used frequently to shut down the internet services but the cost in terms of economy, businesses and jobs has been colossal and has not been adequately considered.

Internet Connectivity and Impact of Competition

The digital businesses claimed that accessibility of high-speed broadband internet was a problem before the arrival of Jio. As fibre lines were not available, to access high speed broadband internet, the businesses had to take a leased line connection from the existing internet service providers. This would cost as much as Rs 40,000 per month. However, after the arrival of Jio, competition increased in the market and internet connectivity enhanced substantially. Now, it became possible for the start-up to get a high-speed broadband internet connection for just Rs 10,000 for a period of three months. Further, the start-up stated that now, it was possible to get high speed broadband internet connection even in the outskirts of the city and in certain remote areas.

From our list of interacted with businesses:

- 12 businesses believe that digital infrastructures are critically important for investment, growth and expansion.
- Eight businesses said that adequate digital infrastructure is important for delivering quality services and nine businesses said that it is important for consumer satisfaction. Digital infrastructure helps them in going innovative to improve the quality of services as well as maintaining better consumer experiences. The business was able to pinpoint some states such as West Bengal, Jharkhand and Odisha where digital infrastructure is not very advanced, which impacts the onboarding of customers and educators and students.



- The businesses also mentioned that **the issue of language barrier in technology and education** stopped the business from onboarding the students from regional languages, particularly students living in rural settings of the country.

Start-up had a unique take on adequacy of **digital infrastructure.** They commented that governments both central and state have brought in various initiatives for encouraging innovation and start-ups. These initiatives include mentorship under Atal Innovation Mission (AIM) and setting up of incubation centres, which have high end computers, high speed internet and co-working space office setup for start-ups in nascent stages. This infrastructure support from government schemes provides motivation and innovation and allows businesses to have a strong footing without giving away resources to infrastructure from the get-go. Further, these incubation centres such as the Bhamashah Techno Hub support the businesses in registration, compliances, introducing them to right investors, introducing them to funders for technology, marketing and networking, which the businesses and their owners might not be aware of due to lack of exposure. The hub provides for mentors to hand hold them through the process of establishing a digital business from scratch.

When these findings were placed before a panel of experts to seek suggestions on addressing the concerns, we received critical inputs. Following is a brief summary of our interaction:

India has done well by setting up the digital rails and creating public digital codes and public digital infrastructure. This has led to a lot of growth that we are seeing currently in digital businesses. India has a large consumer base and carries the potential to become a leader in the digital landscape, which can enhance the ease of living for millions. Innovations such as the Unified Payment Interface (UPI) and the Open Network for Digital Commerce (ONDC) are unique innovations, which showcase the knack for innovation that is already present among Indians. India Stack based digital rails along with other government initiatives like the Government e-Marketplace, Umang App, Digilocker are key developments for digital businesses.

However, the big promise of digital infrastructure "democratisation and increasing participation" has not been fully realised so far and remains very siloed as the cost to plug into it may be too high to be borne by smaller businesses. New business models are being developed around digital infrastructure. Thus, longevity of the digital infrastructure is critical. In addition, regulatory uncertainty around this

infrastructure is also present, which impacts the overall Indian digital economy. For example, the Supreme Court has intervened in operations of Aadhaar. Thus, certain businesses get stopped or their cost of operations increase. Legislative certainty is important for digital businesses that have dependability on the digital infrastructure.

Moreover, mechanisms of capacity building of businesses, particularly for smaller businesses, is currently fairly non-existent and there is a need to provide such mechanisms as it protects consumers as well as helps businesses to grow. Initiatives by the government such as the Atal Innovation Mission, which helps digital start-ups exist need to be expanded. For instance, ultimately ensuring that data of consumers is secure and websites are not leaky buckets of malware needs to be ensured by the businesses. Businesses often rely on consultants who would make a WordPress website for them, but there are insecure WordPress plugins that might cause consumer harm in terms of data breach. Smaller businesses find it difficult to adopt good practices of cyber hygiene due to capacity constraints.

Further, capacity to comply is a huge constraint, regardless of the business being big or small. There is a cost involved not just in terms of spending on compliance but also in terms of opportunity cost. While the market has groomed, our approach to regulating that space has not kept pace. Regulations are being imposed in an ad hoc manner. It is important that businesses are regulated from a place of trust, as doing the contrary will hurdle industry growth. Therefore, capacity building is required prior to the regulation and should be done continuously and simultaneously. Capacity building should include awareness generation about regulations that are busy in ensuring that their revenue streams are maintained. Apart from English and Hindi, awareness should be done in regional languages to make it more inclusive.

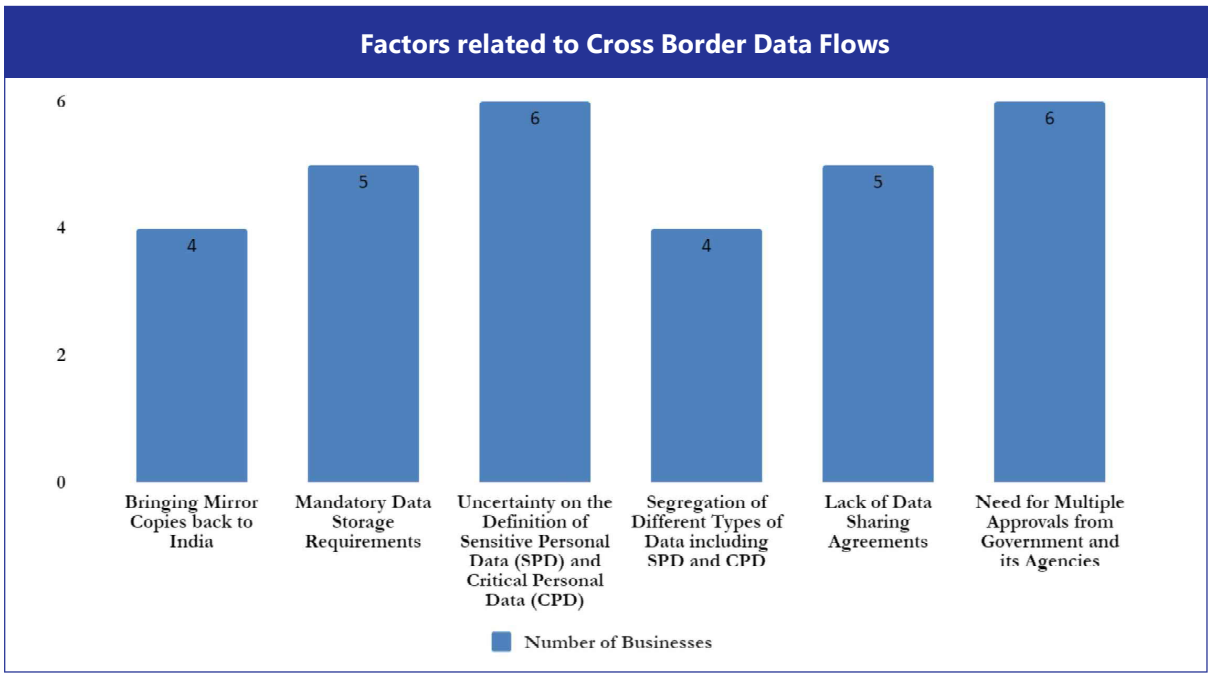
As digital businesses grow exponentially, several issues such as transaction failure and reports of finger print failures have become rampant. The UIDAI has conducted pilot studies wherein, it has found that by utilising simple educating techniques for the operators have helped increase the efficiency of the system and success rates have jumped up by 10-12 per cent. Some of the trivial errors include people putting fingers vertically rather than horizontally and not keeping the plate of the scanner clean where the fingerprint is taken. Grievances can be redressed through mechanisms like toll free number, WhatsApp numbers or email addresses and other online dispute resolution (ODR) mechanisms. Government departments are developing grievance redressal solutions, with citizen charters to resolve grievances in specific time frames.

The challenge in today's digital era of digitally provided services and digital businesses is that there is a faceless entity and one does not know whom to go to for grievances. Grievance redressal options through social media channels like Twitter are good for the ones who can access them. However, if one does not have adequate social capital, the person is left with almost no option. Therefore, for those who are not digitally connected and lack accessibility, having the option of grievance redress officers who can resolve the grievances in person will be more useful. Reinstating responsive feedback loops can be helpful so that it keeps the government abreast with what the general public is facing. A 'digital first access' instead of an 'only digital access' should be the way forward as many people may not have any equipment, either a smartphone or computer to access the digital first grievance redressal mechanism.

E. Cross-Border Data Flow

In the recent past, economic growth has been alarmingly slowing down but the digital economy has been growing exponentially, which now accounts for 15.5 per cent of global gross domestic product.[15] However, legitimate anxieties over surveillance, security, and economic inequality are justifying governmental measures. The issue stemming from data localisation mandates – increasing restrictions on cross-border data flow – poses a critical concern to the future of international trade and digital businesses globally as it erects borders in cyberspace. Data is the lifeblood of international trade in the digital age and is reflected in its contribution to the Information Communication Technology (ICT)-enabled business in global Gross Domestic Product (GDP). McKinsey estimates that worldwide data flows raised 10 percent of GDP globally.[16]

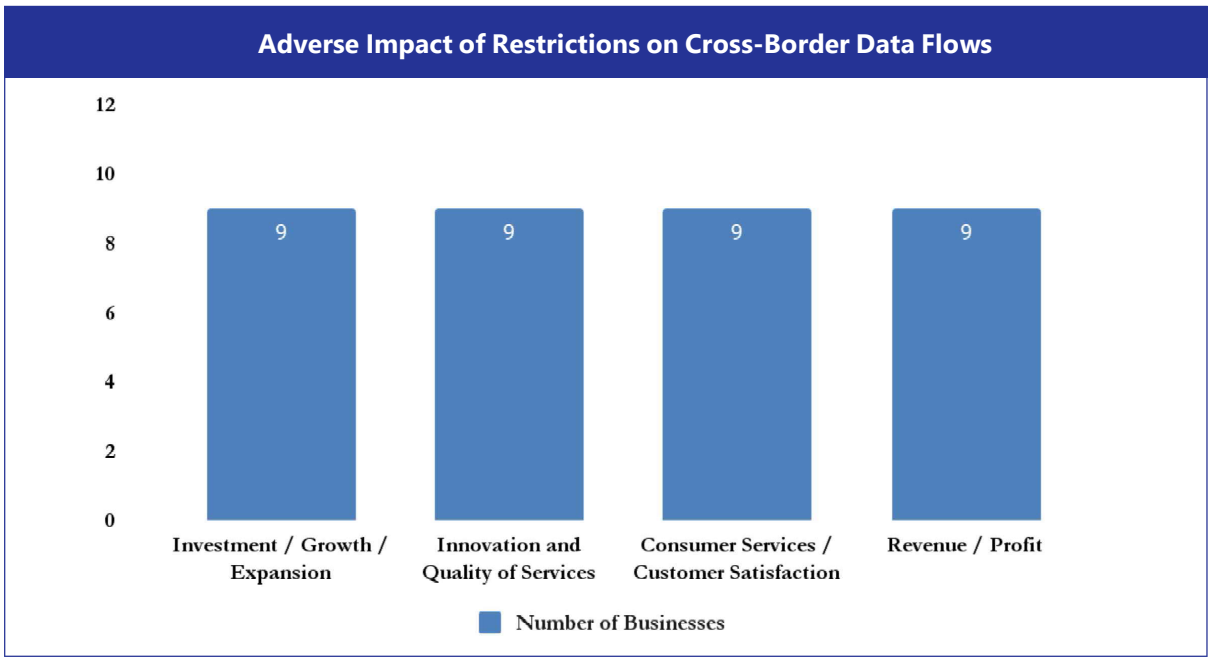
India already has regulations under implementation and has also proposed policies that mandate degrees of restrictions on the cross-border flow of data. In multiple recent documents such as E-



Commerce Policy, Non-Personal Data Governance, Reserve Bank of India (RBI) Notification on Storage of Payment System Data, and the proposed Data Protection Bill, 2021 the Government of India (GoI) makes it clear that India is fast moving toward data localisation. Key considerations for mandating and/or proposing data localisation policies are fostering better economic growth and enhancing security. However, these claims are not backed with clear evidence as the relation between data storage location and value creation is not so clear and costs and benefits also need to be taken into account.[17]

During our stakeholders' interaction on restriction on cross-border data flow, most digital businesses, except an e-commerce platform and an online gaming platform, identified CBDF as one of the most important parameters for EoDDB. However, mixed responses were received on the issue of which kind of existing or proposed regulation related to CBDF or data localisation are or will be cumbersome. Engagement with four businesses revealed that bringing mirror copies back to India is a cumbersome process and might negatively impact doing digital business in the country. Five businesses said that mandatory data storage requirements are not business-friendly and it increases the cost of operation for digital businesses. Smaller service providers operating with limited resources may not be able to differentiate between sensitive personal data and critical personal data and be compelled to store entire personal data with themselves in India.

Six businesses said that definitional uncertainty in critical personal data and sensitive personal data is making them anxious. Only two businesses feel that segregation of personal and non-personal data will not only be cumbersome but also resource intensive. Though, the other businesses have not highlighted the concerns related to segregation of personal data because they are yet to comply with. The limited clarity in definitions such as what constitutes critical personal data, state policy, public policy and national security create uncertainty around compliance.[18] Further, seven businesses believe that the need for multiple approvals from government and its agencies can be a lengthy and time-consuming process and not digital businesses will desire to be in such a situation. For instance, there is no clarity on when the Data Protection Authority (DPA) has to consult the central government about the confidential contracts for data transfer across the borders.[19] This will create a bottleneck in data transferring due to its scale. For data transfer across borders, examining each contract further make the issues problematic as it may contain confidential business contracts.



Nine businesses believe that CBDF is critically important for investment, growth and expansion. Nine businesses said that adequate CBDF is important for delivering quality services as well as consumer satisfaction. Further, nine businesses feel that CBDF helps them to achieve better profits. Nine businesses revealed that lack of data sharing agreements within the country and globally might adversely impact businesses in India. Similar sentiment echoed in CUTS study 'Digital Trade & Data Localisation', which shows the unintended consequence of data localisation on India's Information Technology and Business Process Management Industry regarding digital services export.

Conclusion

We have witnessed that EoDDB issues have manifested themselves in different kinds of technology law and policy developments over the past couple of years. While EoDDB may be necessary, it should not be an exclusive end goal. The end it seeks to achieve needs to be evaluated. It should serve the consumers and the industry alike. Thus, encouraging EoDDB reforms and realising these reforms will act as a means to the end of achieving better living standards for citizens and improving Ease of Living.

Endnotes

1 A part of the interaction with experts is available at The Unease of Doing Digital Business in Digital India

2 https://cuts-ccier.org/pdf/dp-impact-of-criminalising-provisions-on-ease-of-doing-digital-business-in-india.pdf

3 https://cuts-ccier.org/pdf/dp-impact-of-criminalising-provisions-on-ease-of-doing-digital-business-in-india.pdf

4 Ward, Jake, 'Digital big tech drives small business success', November 19, 2019, the Hill, available at https://thehill.com/opinion/technology/471005-digital-big-tech-drives-small-business-success

5 https://www.financialexpress.com/india-news/to-be-tabled-in-winter-session-of-the-parliament-bill-to-decriminalise-110-economic-offences-soon/2707484/

6 https://economictimes.indiatimes.com/tech/technology/india-has-over-450-web3-startups-with-investment-of-1-3-billion-nasscom-report/articleshow/94949763.cms

7 https://twitter.com/i/broadcasts/1eaJbNOoXPZJX

8 https://timesofindia.indiatimes.com/india/govt-takes-leeway-skips-pre-legislative-procedure-on-bills/articleshow/89513634.cms

9 Robertson, Peter J., and Taehyon Choi. "Deliberation, consensus, and stakeholder satisfaction: A simulation of collaborative governance." Public Management Review 14.1 (2012): 83-103.

10 'Compliance brings international consequences for digital business', ZDNET, *available at* https://www.zdnet.com/paid-content/article/compliance-brings-international-consequences-for-digital-business/

11 Ministry Of Corporate Affairs - DIR-3 KYC

12 RBI Notifications

13 Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, *available at* Fat salary but bigger risks: Is this a tech job that nobody wants?

14 Gasparri G. Risks and Opportunities of RegTech and SupTech Developments. Front Artif Intell. 2019 Jul 30;2:14. doi: 10.3389/frai.2019.00014. PMID: 33733103; PMCID: PMC7861216, *also available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7861216/

15 Huiyao, Wang, 08 June 2022, 'A World Data Organisation needed to avoid rules-based disorder', South China Morning Post, *available at* https://www.scmp.com/comment/opinion/article/3180717/world-data-organisation-needed-avoid-rules-based-disorder

16 Aggarwal, A., (2018) Can Data Protection Help national, economic interests. *LiveMint*. Retrieved from https://www.livemint.com/Opinion/P9bGTw36JUx8YTK0RxKGhN/The-economic-impact-of-a-strict-data-localization-regime.html [28 February 2022].

17 Chander, A., & Schwartz, P, 2022, 'Privacy and/or Trade', available *at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

18 Report of the JPC on the Personal Data Protection Bill, 2019. (2021). Retrieved from http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf [24 February 2022].

19 *Ibid*

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org
Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).