June | 2022

Discussion Paper

CUTS International
www.cuts-international.org

Impact of Unnecessary Compliances on 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 framework for regulatory assessment basis the elements of 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.

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]

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]

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]

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]

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

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.

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.

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 And needs to be simplified, amended or repealed.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

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

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.

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.

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.

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.

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.

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 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.

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

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[76][77] 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.

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

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]

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

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.

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.

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

This Discussion Paper was authored by Neelanjana Sharma (njs@cuts.org), Senior Research Associate, CUTS International. The author gratefully acknowledges the contribution of Amol Kulkarni, Director (Research), Prince Gupta, Senior Research Associate and Asheef Iqubbal, Senior Research Associate, CUTS International to this paper.

© CUTS International 2022. This **Discussion Paper** is published by CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER), D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India. Ph: +91.141.228 2821, Fx: +91.141.228 2485, E-mail: c-cier@cuts.org, Web: www.cuts-ccier.org. Also at Delhi, Calcutta and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA).

CUTS Discussion Papers are to inform, educate and provoke debate on specific issues. Readers are encouraged to quote or reproduce material from this paper for their own use, but CUTS International requests due acknowledgement and a copy of the publication.

June 2022