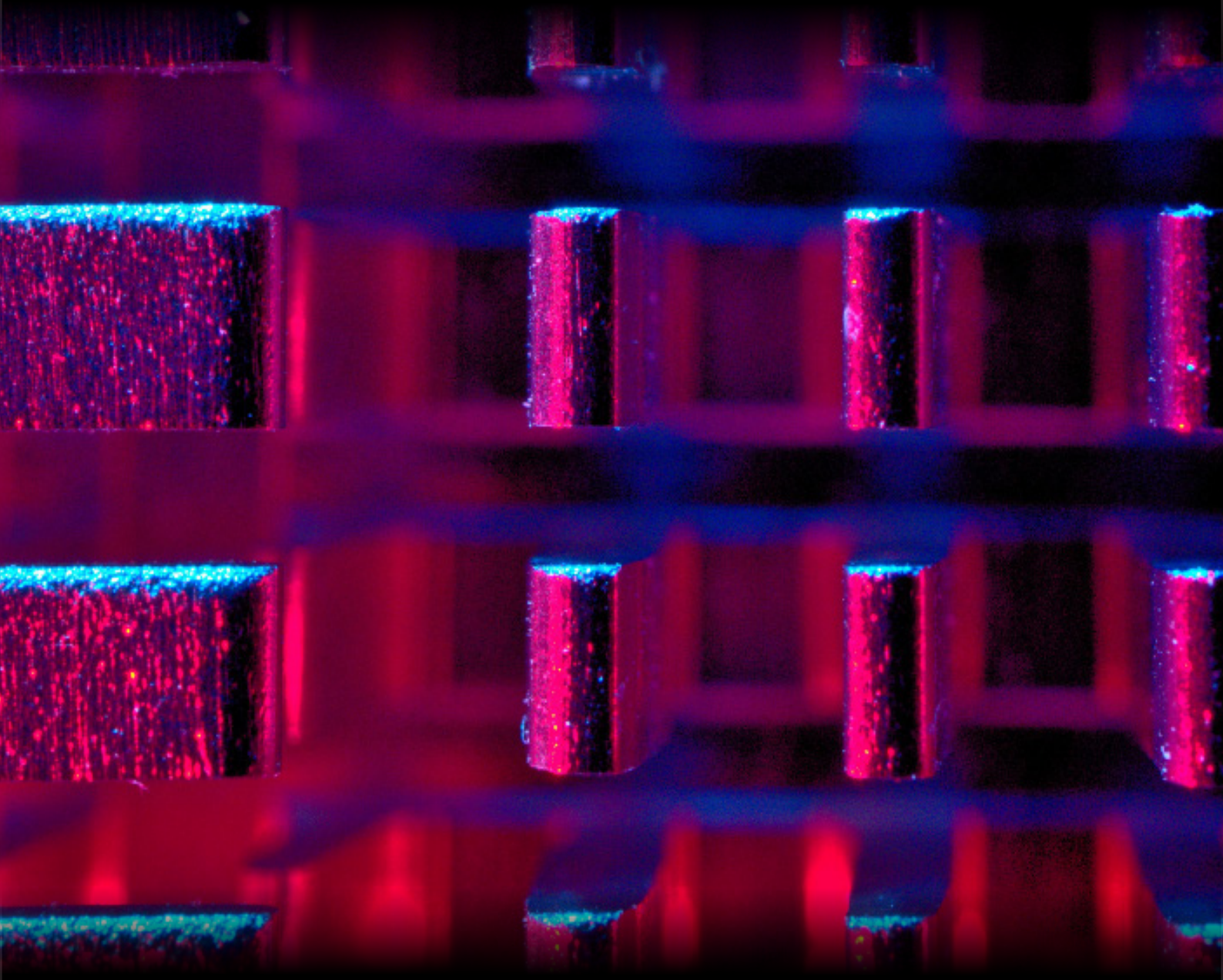
Reimagining India's Information Technology Act



KOAN

May 2021

Authors
Priyesh Mishra, Akshat Agarwal, Mohit Kalawatia, Aditi Chaturvedi

Design
Aadya Agarwal

contactus@koanadvisory.com | www.koanadvisory.com

Table of Contents

List Of Abbreviations

Abbreviations	Expanded Form
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
AI	Artificial Intelligence
APAC	Asia Pacific
CCS	Competition and Consumer Commission
CDA	Communications Decency Act
CECA	Comprehensive Economic Cooperation Agreement
CERT	Computer Emergency Response Team
CIA	Confidentiality Integrity Availability
CMA	Competition and Markets Authority
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSP	Cloud Service Provider
DMA	Digital Markets Act
DPIIT	Department for Promotion of Industry and Internal Trade
DSA	Digital Services Act
DSB	Dispute Settlement Body
DSCI	Data Security Council of India
EARN IT	Eliminating Abusive and Rampant Neglect of Interactive Technologies
EU	European Union
FCC	Federal Communications Commission
FDI	Foreign Direct Investment
FOSTA	Fight Online Sex Trafficking Act
FTA	Free Trade Agreement
FTC	Federal Trade Commission

Abbreviations	Expanded Form
GCI	Global Cybersecurity Index
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IL	Intermediary Liability
IMDA	Infocomm Media Development Authority
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
IPC	Indian Penal Code
IPR	Intellectual Property Rights
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
MEITY	Ministry of Electronics and Information Technology
ML	Machine Learning
MMS	Multimedia Messaging Service
NCCC	National Cyber Coordination Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
NCSC	National Cyber Security Centre
NITI	National Institution for Transforming India
NPD	Non-Personal Data
NSA	National Security Advisor
OISP	Online Intermediary Service Providers
OTT	Over The Top
PDP	Personal Data Protection
PNC	Police National Computer
POFMA	Protection from Online Falsehoods and Manipulation Act

Abbreviations	Expanded Form
SESTA	Stop Enabling Sex Traffickers Act
SG	Singapore
SMAC	Social, Mobile, Analytics and Cloud
TLS	Transport Layer Security
TRAI	Telecom Regulatory Authority of India
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UAE	United Arab Emirates
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
URL	Uniform Resource Locator
US	United States
USD	US Dollar
VPN	Virtual Private Network
WEF	World Economic Forum
WTO	World Trade Organization

Introduction

The Information Technology Act (IT Act) was notified into law on 17 October 2000, bringing into Indian law the United Nations Commission on International Trade Law (UNCITRAL) Model Law on e-Commerce. The IT Act supplies a legal framework for recognising electronic records and digital signatures, defines cybercriminal offences, and provides penalties for the same.1 It also establishes a Cyber Appellate Tribunal to hear disputes under the law.

Over the years e-Commerce activity increased, the outsourcing business boomed, and new forms of online transactions and platforms (and computer misuse) came about.2 This prompted a review of the Act, which in 2008 was amended to introduce provisions governing data protection, intermediary liability and safe harbour. The amendments also expanded the list of cyber offences and gave authorities the power to intercept, monitor or decrypt information,[3] among other changes.

Twenty years after the Act was passed and 12 years since the last major amendment, the state of play in information technology and the internet is dramatically different. The internet now permeates every aspect of Indian society, bringing immense benefits and challenges unforeseen. The rise of data analytics for instance, has changed how businesses operate and make decisions. Data is widely recognised as a new factor of production,[4] engendering concern about information privacy and individual rights.

Social media platforms too have had a significant impact, changing how we consume entertainment, news and information, and birthing the spectre of misinformation and disinformation. These paradigm shifts have created a flux in law and regulation worldwide, as decision makers try to catch up to technology. Being a democratic polity with large inequities in society and economy, India has high stakes in technological development, as endorsed by visionary government programmes such as Digital India. As recently acknowledged by the Union Minister for IT and Electronics, the IT Act is thus ripe for an update.[5]

Changes in the economic role of the IT sector compound the need for legislative amendments. In the early 2000s the sector capitalised on India's endowment of cheap skilled labour to become one of the largest exporters of IT services. Computer services exports grew at an average annual growth rate of 18.1% between 2006 and 2011. However, the business process outsourcing services that accounted for 77% of India's IT/ITeS exports in 2018-19 have gradually become less valuable.[6] New technologies such as machine learning, artificial intelligence and the Internet of Things are now at the forefront of global technological progress, in which Indian companies have only limited participation.

According to NASSCOM only 18% of Indian startups leverage deep tech such as artificial intelligence (AI), machine learning (ML), blockchain and similar technologies.[7] Deep tech companies work to offer fundamental engineering innovations, not always focusing on end-user services, which they significantly impact nonetheless. While Indian IT giants have invested in these technologies, they do not command the same competitiveness as in outsourcing.[8] They are also conceding their labour cost advantage to east Asian economies, and mass layoffs have become a common phenomenon at large Indian IT firms.[9]

Low investment in cutting-edge technologies is exacerbated by the absence of an encouraging ecosystem. In 2018 there were only 1.1 networked devices per person in India, much lower than the 2.1 in the Asia-Pacific or 2.4 in the world.[10] The NITI Aayog has argued that insufficient supercomputing infrastructure in India impedes progress in AI technologies.[11] Legislation to enable investment in risky innovations could make India a global hub of technological progress for the millions of Indians who will join the internet population as connectivity increases. It would also engage Indians (half of whom are younger than 25)[12] in more valuable economic activities, paving the way for India to become a global leader in IT law and regulation, especially among developing countries with similar social and economic constraints.

This report intends to serve as a primer for stakeholders in the process of IT law reform. It reviews the available options and global best practices that any future statutory framework will have to consider. The experiences of other jurisdictions that grappled with the same problems can be valuable; a comparative approach also offers perspectives from various stakeholders in a crowded technology ecosystem, whether companies at the forefront of digital innovation, states with different ideals for the digital economy, or individuals whose rights are at stake.

The jurisdictions studied here offer wide ranging perspectives. The report evaluates legal frameworks from the United States, United Kingdom and the European Union in view of the impact their laws have had on the global technology discourse. It analyses developments in Germany, Australia, Singapore and Japan as jurisdictions that took unique approaches to specific problems: such as Germany's success in building state capacity to effectively intercept communications. Finally, the experience of Brazil as a developing economy with a landmark digital rights framework, the Marco Civil da Internet, offers important insights.

We also consider the different regulatory approaches a future framework could incorporate. One such choice is between regulation based on rules or goals. Rules based regulation is a system of prescriptive rule making that aims for precision and certainty: it requires greater expertise from regulators and places more responsibility on them. Goals based regulation sets out principles or standards to achieve, while permitting greater flexibility in how to achieve them. A newer approach, it is better suited to innovative and fast-moving sectors with high market change and multiple risks. The suitability of either approach will be determined by contextual factors such as the nature of risks, regulatory capacity, and the degree of innovation and change. Rarely do states implement a pure version of either, with most approaches being hybrids in different proportions.[13]

Such a hybrid approach to regulation will likely be seen across the Indian digital ecosystem, with the IT Act serving as the basic law (or rule based element) applicable to all entities in the online ecosystem. The goal based element may take the form of self regulatory efforts led by industry, in line with certain desired regulatory outcomes in specific areas such as content regulation, or the regulation of a specific segment such as fantasy sports.

Similarly, a choice must be made between a centralised framework with a single body exercising regulatory control, and a more dispersed framework for various sectoral regulators' IT related functioning. These decisions will have to factor Indian particularities: the need to become a hub of IT knowledge and innovation, limited state capacity, and the need to protect and promote the growth of small and medium businesses.

The chapters are arranged thematically: covering e-Commerce, intermediary liability, data governance, encryption and law enforcement access, access and blocking, and cybersecurity.

I. e-Commerce

KEY TAKEAWAYS

- The IT Act in its current form lacks a clear definition of e-Commerce. Other legal documents such as the FDI Policy and proposed e-Commerce policy do not define the term consistently.
- Innovative business models in the digital sphere require workable definitions in legal documents that single out the intended e-Commerce businesses and avoid an outdated, one size fits all approach.
- There is no clear demarcation of the jurisdictional remits of multiple existing and proposed regulators for e-Commerce in India. By contrast countries such as the US, Singapore and Australia have fewer regulators and clear jurisdictional bounds.
- Regulatory certainty is crucial for business continuity. India may consider a vertical approach to regulations instead of the existing horizontal approach.

I.1. Opportunity for India

Electronic or e-Commerce refers to domestic or international commerce in which internet or internet based technology providers source, administer, and/or deliver goods and services physical or digital. It may mean ordering a product from an e-retail website, booking tickets or hotel rooms through travel portals, and using communication channels such as email or voice over internet protocol. It also includes media and entertainment content provided through streaming services, and electronic banking transactions.

The transformational impact of e-Commerce in India can be attributed to the unprecedented adoption of smartphones, a young and tech savvy population, and affordable access to internet services. These advantages have also given rise to a startup ecosystem in India.

Unfortunately, our regulatory architecture has been slow to catch up to this tech-fuelled entrepreneurial spirit. The importance of a clear and cogent framework to regulate these activities cannot be emphasised enough. Such an architecture is needed to ensure certainty for domestic and international players who want to invest in India's burgeoning digital economy. Recognising this, the Union Ministry of Electronics and Information Technology (MeitY) has set a target for India to become a USD 1 trillion dollar digital economy by 2025.

India needs a contemporary framework for the regulation of e-Commerce

I.2. The IT Act

The preamble to a law is useful to decipher its legislative intention. The preamble to the IT Act states that it is:

"an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce"

Although it gives recognition to e-Commerce, the Act contains no clear definition of the term. The preamble, which states that e-Commerce involves the use of alternatives to paper based methods of communication, information storage, and to facilitate the electronic filing of documents with government agencies, fails to reflect a modern understanding of e-Commerce.

The preamble to the IT Act only makes vague reference to e-Commerce

The Act does not define e-Commerce

I.3. Scope of e-Commerce

I.3.i Varying definitions of e-Commerce

The expansive scope of e-Commerce can be understood from international trade negotiations. Since the establishment of a Work Programme on e-Commerce at the World Trade Organisation (WTO) in 1998, e-Commerce related issues have started emerging in bilateral and plurilateral trade agreements. International agreements such as the Comprehensive and Progressive Trans-Pacific Partnership (TPP),[14] the US–Japan Digital Trade Agreement,[15] and the Japan–Mongolia Free Trade Agreement[16] address a wide range of relevant issues, including data protection, consumer protection, competition policy, intermediary liability and cybersecurity.

Regulators in India, however, use the term e-Commerce differently across legal instruments (Table 1) because it is not defined in the IT Act. Consequently there is a degree of uncertainty about the scope of e-Commerce and the applicability of the relevant rules or laws.

Table 1: Definition of e-Commerce in Different Regulations

Regulation	Definition	Implication
Foreign Direct Investment (FDI) Policy	Defines e-Commerce as the 'buying and selling of goods and services, including digital products over electronic or digital networks'.	Exclusive focus on 'buying and selling' means that most digital services intentionally or unintentionally remain outside the ambit. For example, when a consumer purchases an operating system, she merely gets a licence to access that software for a particular period. There is no transfer of ownership, which is a key element of sale.
Consumer Protection Act of 2019	As the FDI Policy was one of the first legal instruments to define the term, subsequent legislations including this Act have adopted the same definition.[17]	First, like the FDI Policy, it is narrow in scope. Second, unlike the FDI Policy, the new Act fails to factor in distinct business models operating within its scope.
Draft e-Commerce Policy	Defines e-Commerce to include the buying, selling, marketing or distribution of goods, including digital products and services, through electronic networks.	The draft policy adopts a broader definition of the term.[18] As a result, transactions, monetary or non-monetary, sale or licence, fall in its ambit. This is in line with the approach adopted at the WTO (see Box 1).
Central Goods and Services Tax Act of 2017	The term electronic commerce is defined to mean the supply of goods or services or both, including digital products, over a digital or electronic network.	The term supply is defined to include all forms of supply of goods and services, such as sale, transfer, barter, exchange, licence, rental, or lease. The definition is wide in its scope as it includes a larger segment of business models that leverage an electronic network, typically the internet, to conduct business.

Box 1

e-Commerce under the WTO's Work Programme

The WTO's Work Programme[19] defines e-Commerce as 'the production, distribution, marketing, sale, or delivery of goods and services by electronic means'. In other words, this definition brings within its purview all aspects of activities carried out over the internet.

Different regulations define e-Commerce differently in India. This creates confusion among market participants.

I.3.ii Ambiguous definition of digital products

Another gap in India's approach to e-Commerce is the ambiguity in defining the term 'digital products'. Several legal instruments and policy proposals including the IT Act, FDI Policy and Consumer Protection Act 2019 do not define the term. The Draft e-Commerce Policy mentions 'digital product' but does not clarify what goods or services fall under the category.

The only legal definition of digital products is found in trade agreements such as the India-Singapore CECA.[20] It is similar to the definitions found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership,[21] the Korea-US FTA[22] and the Singapore-Australia FTA.[23]

The India-Singapore CECA provides that 'digital products' include computer programs, text, video, images, sound recordings and other products that are digitally encoded, regardless of whether they are fixed on a carrier medium or transmitted electronically. The agreement contains a footnote clarifying that the term does not include digitised representations of a financial instrument. Similar definitions are found in the trade agreements mentioned above.

The absence of a definition of digital products in IT legislation leaves it open to varied interpretations. For example, it is unclear if additive manufacturing (colloquially known as 3D printing) will be categorised as a 'manufacturing activity' or a digital product under the FDI Policy. The relevant compliances under the FDI Policy will depend on its categorisation.

In this context, India may consider defining digital products to mean goods or services that can be consumed only in electronic or digital format – which includes text, video, software programs, images and sound recordings. We further recommend that a negative list be created (which can be amended when required) listing out the products that do not fall within the ambit of 'digital products'. This would give the government the requisite flexibility to incorporate 'products' that were not envisaged to be regulated.

Several legal instruments and policy proposals do not define digital products. This lack of definition troubles compliance with the FDI Policy.

Digital products should be treated distinctly from physical goods. To this end, India may consider formulating a negative list that can be revised periodically.

I.3.iii Impact of broad definitions on e-Commerce

The absence of definitional focus in the IT Act has several unintended consequences. For instance in 2018 the MeitY released the Draft Intermediary Guidelines (Amendment) to tackle the social media misuse and the spread of fake news. However, the Rules proposed in the Guidelines do not apply only to social media platforms, but also to other e-Commerce players in the digital ecosystem such as cloud service providers.[24] This is because the sweeping definition of an 'intermediary' in the IT Act[25] includes internet service providers, cloud service providers and cyber cafes. This raises several concerns.

For instance, Rule 3(9) of the Guidelines proposes that intermediaries must deploy automated mechanisms 'for proactively identifying and removing or disabling public access to unlawful information or content'. Complying with these requirements may not be feasible for intermediaries like cloud service providers or CSPs. Unlike social media platforms, CSP infrastructure is typically used by businesses and governments for commercial purposes, governed by bilateral contractual terms with strict confidentiality obligations. Deploying automated tools to monitor such content could violate these contractual terms and conditions.

Regulations that attach liability to vast groups as a homogeneous class run the risk of creating a disproportionate liability framework. Seeking to account for all scenarios they inadvertently make the law rigid, and unresponsive to technological or business model specificities.

One way to mitigate the risk is by crafting workable definitions in legal documents focused on specific e-Commerce businesses. To illustrate, MeitY is reportedly working to introduce a distinct definition for social media platforms so as to limit the applicability of the proposed amendments.[26] Similarly, the Personal Data Protection Bill 2019 contains a definition of social media intermediaries and allows for the creation of certain distinct obligations for such intermediaries.

The absence of a cogent definition of 'e-Commerce' in the IT Act results in multiple and ambiguous regulations. Businesses can find it impossible to comply with these rules, which were not designed for them.

I.4. Jurisdictional Clarity

The overlap of subject matter between Ministries leads to ambiguous jurisdictional boundaries. According to current government rules[27] the Department for Promotion of Industry and Internal Trade (DPIIT) is entrusted with all matters relating to e-Commerce.[28] However, administration of the IT Act, which provides legal recognition to e-Commerce, lies with MeitY. Moreover the Department of Telecommunications has been vested with policy, licensing, and coordination matters relating to telegraphs, wireless, and data.[29]

The result of these overlaps is that several government bodies have framed their own regulations to govern e-Commerce. This leads to disputes over supervisory roles and confusion among market participants over the applicability of legal instruments.

An example of such regulatory overlap[30] is the DPIIT's Draft E-Commerce Policy, which touches on issues relating to community or non-personal data, and consumer protection. It proposes several rules intended to regulate data-sharing practices among businesses. The IT ministry was reportedly of the view that issues of data protection and sharing should be kept out of the e-Commerce policy.[31] In 2020 an Expert Committee established by the MeitY[32] recommended[33] the creation of a distinct Non-Personal Data Authority to regulate non-personal data, in addition to the Personal Data Protection Authority proposed under the Personal Data Protection Bill. The Union Consumer Affairs Ministry has also now issued guidelines for consumer protection in digital space.[34]

Similar issues can be seen in other sectors. In 2018 the Telecom Regulatory Authority of India (TRAI) published a consultation paper on over-the-top or OTT communication services, to explore the possibility of regulating such services through the licensing conditions used for the telecom sector.[35] Multiple stakeholders pointed out in their response to the Authority that these matters fall largely within MeitY's domain.[36] TRAI in its recommendations of 14 September 2020 decided not to impose licensing conditions on OTT services.[37] However, it left open the option of future regulatory intervention.

It is indeed a challenge to address the problems emanating from e-Commerce transactions because multiple Ministries have various concerns about the same subject. But if each regulator were to impose its own set of rules most businesses would find it too burdensome to do business online, especially if these rules were not uniform. Nor is there a silver bullet or quick fix, because e-Commerce business models change rapidly. Therefore, the Government should make concerted efforts to clarify the supervisory role of its departments and regulators.

Here the regulatory approaches of the US, UK, Singapore and Australia as explained in Table 2 may serve as useful guides to avoid overlap. In contrast to India these countries have few regulators and clear jurisdictional remits.

Table 2: Regulatory Approaches

Jurisdiction/ Issue	Intermediary Liability	Competition	Consumer Protection	Data Protection	Cybersecurity
India	MeitY; proposed e-Commerce regulator (DPIIT)	Competition Commission of India; and DPIIT (through FDI Policy)	Ministry of Consumer Affairs; DPIIT; proposed e-Commerce regulator	MeitY; Proposed Data Protection Authority	CERT-In and NCIIPC, other non-statutory bodies such as NSA/NCSC, and NCCC
United States	Federal Communications Commission (FCC)	Federal Trade Commission (FTC)	FTC	FTC	Cybersecurity and Infrastructure Security Agency
United Kingdom	Office of Communications (Ofcom)	Competition and Markets Authority (CMA)	CMA	Information Commissioner's Office	Ofcom, and National Cyber Security Centre (advisory role)
Singapore	Infocomm Media Development Authority (IMDA)	Competition and Consumer Commission (CCS)	CCS	Personal Data Protection Commission (part of the IMDA)	Cyber Security Agency of Singapore
Australia	Australian Communications and Media Authority (ACMA)	Australian Competition and Consumer Commission (ACCC)	ACCC	Office of Australian Information Commission	Australian Cyber Security Centre

Definitional clarity and clear jurisdictional boundaries are foundations for the third crucial aspect governing e-Commerce in India: regulatory certainty

I.5. Regulatory Certainty

Regulatory certainty is critical for business continuity and a key fillip for digital businesses. Regulation in the form of complete bans, onerous licensing requirements, or registration obligations negatively impacts consumer welfare as well, by distorting demand and consumer choice.

I.5.i Unsuitable traditional regulatory models

Digital-driven businesses face a variety of challenges from traditional regulatory models.[38] These include coordination problems, regulatory silos, and the application of outdated rules. The ability of online businesses to evolve and shift from one regulatory category to another makes it difficult for them to operate in a rigid regulatory setup. For example, if a restaurant aggregator begins delivering pre-packaged food products, it may come under the jurisdiction of the weights and measures authority. If it uses drones for delivery, it may come under the jurisdiction of aviation regulators.

Regulatory uncertainty impacts businesses and customers. Traditional regulatory models are not suited for digital-driven businesses. Many of these are not compatible with shape-shifting businesses.

Where industry regulators decide on higher levels of regulatory intervention, there is a loss in the overall competition in the market due to the suppression of technological change.

The International Telecommunication Union (ITU), while investigating regulatory approaches for digital businesses[39] noted that 'even where industry regulators decide on higher levels of regulatory intervention, history indicates that restrictions placed by governments on technological advances are difficult to maintain and cannot be sustained in the long run'. The ITU also emphasised the loss in overall competition in the market caused by the suppression of technological change.

The innovative business models of e-Commerce entities face several legal challenges when they fall within overlapping sectoral jurisdictions. A search engine may be required to comply with the data protection framework for its data collection and sharing practices, with advertising and consumer protection law for its advertising functions,[40] and safe harbour protection in IT law. Most innovative e-Commerce creates such concerns and disrupts the rigid application of traditional laws.

In this context the ITU offers four principles to achieve optimum regulatory outcomes:
(a) harmonise regulations regionally and globally,
(b) acknowledge the shift to Internet Protocol or IP services,
(c) regulate for a new competitive paradigm, and
(d) accept the need for collaborative regulation between other sectoral regulators.[41]

Decision-makers in India do recognise the importance of a harmonised and collaborative rule-making approach. In 2018 the Government constituted a Standing Group of Secretaries to facilitate an inter-ministerial consultation on issues relating to e-Commerce.[42] Government arms such as the DPIIT, the Ministry of Consumer Affairs, the Micro, Small and Medium Enterprises Ministry, and the Ministry of Finance participated in the process.

Despite this, a piecemeal approach to regulation persists, as described in Box 2.

This does not mean, however, that a unitary mechanism or one size fits all approach should be adopted to govern e-Commerce businesses. Rather, the Government can explore sector-specific rules that encourage innovation. For example, a comprehensive data protection framework is critical to protect the fundamental right to privacy. The sectoral data protection provided for in the Personal Data Protection Bill 2019 is one such example.[46] While the Bill lays down penalties for contraventions, it does not restrict business operations.

Box 2

Regulation of Online Pharmacies

In August 2018 the Ministry of Health and Family Welfare issued a set of draft rules for regulating e-pharmacies in India.[43] The draft rules required all entities intending to conduct the business of e-pharmacy in India to seek registration from the Union government.

The sale of pharmaceutical drugs in India is regulated under the Drugs and Cosmetics Act of 1945. As per the Act, a licence is required to sell all drugs except those listed in Schedule K of the Drugs and Cosmetics Rules of 1945.[44]

The 2018 draft sought to extend rules applicable to offline pharmacies to online pharmacies. It did not take into account the 'marketplace model', whereby an e-pharmacy merely acts as an electronic delivery platform between a licensed pharmacy and a consumer.

The draft rules are yet to be finalised; in the absence of a legal framework, some e-pharmacies in India are operating as technology platforms under the IT Act.[45] The business operations of online pharmacies could be severely restricted if the draft rules were implemented in the current form. A vertical approach by contrast would ensure regulatory certainty, allowing businesses to operate.

I.6. The Future Imperative

India could consider a vertical approach to regulation, rather than the existing horizontal approach. A vertical approach is one that empowers sectoral regulators to create rules affecting those within their regulatory remit, with principal legislation such as the IT Act to provide overarching legal certainty. The system is supposed to ensure a healthy division of work, with each level of government doing what it does best. In a horizontal approach, each sectoral authority works in a silo, due to a lack of definitional clarity and blurred jurisdictional boundaries, which results in conflicting legislations erecting regulatory barriers to digital commerce.

A vertical approach can improve efficiency in the policymaking process. For example, the consumer authority would continue to set consumer welfare standards, the data protection authority would formulate standards for data collection, analysis, processing and sharing, etc. This enhances operational certainty for businesses, allowing innovative firms to seamlessly shift business practices.

Decision-makers in India recognise the importance of a harmonised and collaborative approach to rule-making, but a piecemeal approach to regulation still persists.

India should consider a vertical approach to regulation that could improve efficiency in the policymaking process. To this end the IT Act could provide legal recognition to digital businesses, while disparate areas like privacy and competition are governed by sectoral authorities.

II. Intermediary Liability: Making Platforms Accountable

KEY TAKEAWAYS

- The global paradigm of intermediary liability is changing from a safe harbour approach to attaching greater responsibilities to intermediaries.
- Regulation of intermediary liability must strike a balance between holding intermediaries accountable and allowing them to innovate and grow.
- There is a need for clear definition and demarcation of various types of intermediaries for effective rulemaking.
- While specific issues such as the spread of misinformation, disinformation and revenge porn can be tackled through specific laws, such laws must be designed to balance internet restrictions and internet freedoms.
- Where pure self-regulation is not possible, India should take appropriate and proportional measures through co-regulation. For issues with implications for democratic integrity and people's security, state involvement may bring greater accountability.

The diversity of intermediaries is a challenge in developing a suitable regulatory framework. Different jurisdictions give intermediary status to different services, such as internet service providers, content services, storage services, and some such as India, even to cyber cafes. But these entities play very different roles in the internet value chain: cyber cafes offer physical access to computers connected to the internet, ISPs provide the actual connection or carriage services (to cyber cafes as well) and online platforms provide digital products and services. These differences make a one size fits all approach unsuited to defining and regulating intermediaries. An update is called for in Indian law around intermediary liability as it currently exists in the IT Act.

There is also a specific concern relating to online social media platforms, which have emerged as economic powerhouses driven by the data ecosystem. These platforms have undoubtedly benefited from the intermediary liability (IL) law, which protects them from third-party liability. It has led to their uncontrolled expansion and unforeseen economic, social and political disruptions. Examples include political or social instability caused by misinformation, online piracy, and the circulation of child sexual abuse material[47] or terrorist recruitment material.[48]

To address these issues, states have begun thinking about new regulatory frameworks. Several have diluted strict IL protections, introducing liabilities based

on the types of platform, their thresholds, and specific issues such as fake news or revenge porn. Some are even considering co-regulation as a preferred model,[49] wherein the state works together with industry to enforce rules. This may have the potential to overcome the lack of accountability arising from self-regulation, and the fear of loss of innovation caused by rigid rules-based regulations. Co-regulatory models may see governments playing a role in facilitation or oversight, or may simply consist of self-regulatory measures with a legal underpinning.[50]

This chapter gives a brief account of the IL regime, the inability of social media platforms to address pressing issues in society, changes proposed by different countries in response to this challenge, and the guiding principles of the co-regulatory model, which could serve as a long term solution for accountability.

II.1. The Genesis of Intermediary Liability Law

Section 230 of the Communications Decency Act (CDA), one of the first laws in the world that dealt with intermediary liability, was passed in the USA in 1996 when the internet was still in its infancy. The provision's rationale was that if intermediaries were held responsible for third party content, they would have to moderate all content. Such a burden would divert resources they would rather invest in growth and innovation. It could also stunt the internet's potential as an emancipatory technology and limit the creation of better products and services. Thus, the first generation of laws addressing intermediary liability prioritised the growth of the internet as a medium for communication and commerce. The focus was on providing safe harbour to intermediaries if they had no intention or knowledge of offending third-party content.

In addition to the CDA, Section 512 of the Digital Millennium Copyright Act provided safe harbour to intermediaries for copyright-infringing content. Most jurisdictions followed suit, granting wide exemptions to intermediaries from liability in the early years. . The European Union's E-Commerce Directive adopted in 2000 contained the key intermediary liability principles of the EU. Its overall goal was to foster the development of e-Commerce in the EU and ensure free movement of 'information society services' between member states. Here, safe harbour was granted to three categories of entities: mere conduit service providers or ISPs, caching providers that temporarily and automatically store data for transmission efficiency, and hosting providers that allow users to store data.

With the increasing scope of problems such as violent and sexually exploitative content, and widespread intellectual property rights infringements, this attitude has changed. Tackling these issues requires a rethink on the part of all stakeholders, on how to approach the responsibility of intermediaries.

At the same time, many platforms now have tens of millions of users and wield considerable power and influence. This has led to discussions on the need to impose greater accountability on social media intermediaries such as Facebook or Twitter. Illustratively, the US recently passed the FOSTA-SESTA package[51] which dilutes Section 230 of the CDA with the objective of targetting online conduct promoting or facilitating sex trafficking. Another proposed American law, the EARN IT Bill,[52] aims to create a code of best practices against child sexual abuse material that intermediaries must follow to retain safe harbour.

These changes have been criticised by advocates of internet freedom, who say they could result in excessive censorship, end internet privacy and overturn encryption.[53]

On 28 May 2020 US President Donald Trump signed an executive order[54] seeking to restrict the scope of safe harbour available to social media platforms, mainly by calling for a new interpretation of the 'Good Samaritan' clause in the CDA. This clause protects platforms from liability for good faith attempts at moderation, even if the moderated content is constitutionally protected. After Twitter flagged two of his tweets as factually false, Trump alleged political bias, and the executive order seeks new rulemaking to define the extent of 'good faith' in moderation practices.

While there is some doubt among experts about the legal validity of this executive order,[55] the American approach is shifting to require more from platforms. In fact in June 2020 the Department of Justice proposed changes to the immunity given to online platforms. These are based on principles intended to ensure that 'tailored changes to immunity to make the internet a safer place would not unduly burden large tech companies', preserve competition, retain core immunity for defamation to preserve free speech, and distinguish between hosting defamatory content and content that facilitates or constitutes federal criminal activity.[56]

While most jurisdictions granted wide exemptions to intermediaries from liability in the early years, there is a move to impose greater accountability on them due to increasing violent, terroristic, and sexually exploitative content, and widespread infringements of intellectual property rights.

II.2. Intermediary Law in India

Under the IT Act, intermediaries are shielded from liability for illegal content posted by third parties, as long as they had no knowledge of its illegality and exercised due diligence. An online platform's liability for content posted on it by users first became a topic of discussion in 2004, when a clip of an infamous MMS scandal was posted for sale by a user on Baazee.com, an e-Commerce platform owned by eBay. In 2008 the IT Act was amended and a more detailed section on IL replaced the old one. In 2011, Intermediary Guidelines were introduced to further clarify the 'due diligence' required of intermediaries. This introduced a standard of notice and takedown, under which platforms are bound to take down content deemed to have violated intellectual property rights, or that is otherwise unlawful, upon receiving the prescribed notice.

Despite revisions, Indian IT law is inadequate to contend with new challenges. It continues to define an intermediary widely and without functional distinctions, leading to confusion about the intended outcomes of rules proposed to tackle challenges such as hate speech and disinformation. In July 2018 the

Union Minister for Information Technology told Parliament about the rising instances of violence because of fake news, saying there was a need to strengthen the implementation aspects of Section 79 of the IT Act, which deals with IL.[57]

The Government proposed new Draft Intermediary Guidelines (Amendment) Rules in 2018 to pin greater responsibility on intermediaries. These create several new obligations, such as a rule requiring intermediaries to ensure the traceability of messages on their platforms, and a rule mandating automated filtering of unlawful content. The Government has also demanded greater cooperation from end-to-end encrypted communication apps such as WhatsApp in tracing the origins of fake news.[58] Civil society organisations have expressed concern that proactive filtering obligations will lead social media platforms to err on the side of caution by over-censoring, rather than risk penalties, leading to reduced freedom of speech online. While there is an undeniable need to impose greater responsibility on online intermediaries, states like India are struggling to find a balanced solution.

Therefore, while existing intermediary liability approaches need updating, the process of reforming them remains unclear. The question impacts several individual rights including the right to free expression. It also affects the right to privacy, recently held by the Supreme Court to be a fundamental right under the Constitution.[59]

Table 3: Benefits and Challenges of Popular Intermediaries

Type of Intermediary	Benefits	Challenges
Social media platforms (Facebook, Twitter, etc)	Easy communication and community building, facilitate free speech, a marketplace of ideas	Hate speech, political propaganda, disinformation and misinformation
Content hosting platforms (YouTube, TikTok, etc)	Provide a platform for creativity and expression, give rise to new creators and a digital creative economy	Copyright infringing materials may be shared and circulated, or unlawful content such as child sexual abuse material, violent content, or terrorist propaganda and recruitment videos
End-to-end encrypted communication platforms (WhatsApp, Telegram, etc)	Secure communications protect privacy by making the illegitimate interception of messages impossible	Law enforcement agencies have trouble monitoring and intercepting these communications, benefiting criminals

As seen in the above table, intermediary regulation requires policymakers to ensure a balance between the benefits wrought by these intermediaries and the concomitant challenges. Additionally, any legal changes are bound to affect technological innovation and economic growth.

Given the various types of intermediaries and differences in the issues they face, policymakers may want to choose between the following two approaches. First, regulation that is premised on a taxonomy of the different kinds of intermediaries. Alternatively, regulation that is made through specific laws dealing with a singular issue, for instance fake news. Some of these best practices are analysed below.

While current intermediary liability frameworks need to be updated, a balanced approach is required

II.3. Best Practices

II.3.(i) Laws based on types of intermediaries

India's IT Act follows a one size fits all approach to regulating intermediaries. Its expansive definition of an intermediary[60] covers everything from social media platforms to internet service providers and cyber cafes. But intermediaries are heterogeneous, with varying degrees of control over the content transmitted through them. The set of tools and mechanisms available to a cybercafe operator are different from an ISP who operates at scale. Similarly, while the operator of a social media platform can remove content from it, an ISP cannot do so.

Several jurisdictions differentiate between classes of intermediaries. This gives regulators the flexibility to frame rules that are goal-oriented and calibrated accurately.

Table 4: Laws based on Broad Classification of Intermediaries

Jurisdiction	Law	Differentiation of Intermediaries
Germany	Telemedia Act	Applies to 'providers of electronic information and communication services' except when they are providing telecommunication services. The Act distinguishes between content and carriage.[61]
Australia	Telecommunications Act	Separately defines 'carriage service providers' and 'content service providers'.[62]
European Union	Digital Services Act, Digital Markets Act	The DSA applies to all Online Intermediary Service Providers (OIPs) offering services within the EU (including internet access providers, domain name registrars, cloud and web hosting services, online marketplaces, app stores, collaborative economy platforms and social media platforms) irrespective of their establishment or residence, and places enhanced obligations on platforms with more than 45 million users.[63] The DMA contains a separate definition for 'gatekeepers' i.e. platforms such as Amazon, prohibiting them from using competitors' data to their advantage, and enforces interoperability and data portability for consumers.[64]

II.3.ii Laws based on threshold limits

The IT Act is an omnibus law that deals with various issues relating to the internet. However, several countries have imposed threshold limits on intermediaries defining the point at which such laws can apply to them.

Some threshold limits are an acknowledgment of the network effects that play out on large social media platforms.[65] The influence and impact of social media sites multiply with a larger number of users, and it is important to tailor intermediary liability obligations accordingly. For instance, Germany's Netzwerkdurchsetzungsgesetz (NetzDG) applies to social network platforms with more than two million users. NetzDG imposes an active obligation on large entities to take down content deemed 'manifestly unlawful' within 24 hours. The law has been opposed by activists who say it is tantamount to forcing companies to censor on behalf of the government, and will lead to unaccountable and overbroad censorship.[66] In the Indian context such a law, so far as it places an obligation upon platforms to make decisions about the

legality of content, would fall foul of the judgment of the Supreme Court in *Shreya Singhal v Union of India*. Here, while striking down a provision in the IT Act,[67] the Court said that competent public authorities and not private companies such as the ones running these platforms should be in charge of making decisions about the legality of content.[68]

The European Commission announced similar threshold based obligations in December 2020. If passed, the Digital Services Act would introduce new requirements for platforms, especially those with more than 45 million users each (designated as Big Tech). It includes algorithm transparency requirements so users can know the main parameters used to rank content, as well as risk assessments for potentially illegal content. Fines of up to 6% of turnover can apply in case of failure to comply.[69]

Attaching greater obligations to large entities ensures that smaller players are not unduly burdened with onerous obligations, while harm is regulated on the biggest platforms. Conversely, if multiple jurisdictions impose different thresholds, it could become harder for smaller companies to expand into the global market. A multiplicity of compliance requirements may prevent the rise of the next Facebook or Twitter, strengthening the existing players' hold on the global market.

To prevent such outcomes, thresholds or norms may be harmonised via international treaties or agreements. A parallel to this principle is seen in global discussions on digital taxation: the Organisation for Economic Cooperation and Development is currently in the process of formulating threshold limits for states so they can levy taxes on digital goods and services.[70]

II.3.iii Laws based on specific issues

Unlawful content

Many states have also passed laws specific to certain issues of online intermediaries. Australia passed the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act in 2019 shortly after the Christchurch mass shooting. The law makes it an offence for an ISP or social media service provider to fail to report and remove material that they think records or streams 'abhorrent violent conduct' that occurred in Australia.

Both the NetzDG and the Criminal Code Amendment also make a distinction based on the gravity or offensiveness of the material in question. In India, after an intermediary receives 'actual knowledge' in the form of a government notice or court order relating to unlawful content, or 'specific knowledge' in the form of a notice of infringement from a particular rightsholder, it has 36 hours to remove the content in question. In Germany on the other hand, a social media intermediary would be required to remove content that is 'manifestly unlawful' as defined under NetzDG within 24 hours. If the content's illegality is not obvious, it has up to seven days.[71] The absence of a strict legal standard or guidelines to determine what counts as obviously illegal is problematic, as it shifts the burden of making what is essentially a judicial decision onto the platform.

Table 5: Takedown Requirements

Jurisdiction	Takedown Requirements
India	• On receipt of 'actual knowledge' in the form of a government notice or court order relating to unlawful content – 36 hours • On receipt of 'specific knowledge' in the form of a notice of infringement from a copyright holder – 36 hours.[72]
Germany	Once a social media platform receives a complaint through a complaint mechanism it is required to set up: • Content that is 'manifestly unlawful' – 24 hours • All other cases of illegal content – 7 days
Australia	Not removing 'abhorrent violent material' (material that depicts acts of terror, murder, rape or kidnappings) 'expeditiously' is an offence. While there is no defined timeframe, the Explanatory Memorandum states that 'the type and volume of the abhorrent violent material, or the capabilities of and resourcing available to the provider' may be relevant factors. Additionally, in the second reading speech, which courts can use to interpret the law, the Attorney-General condemned the fact that video of the Christchurch shooting was broadcast without any interference for 17 minutes, and that it was available for almost an hour and ten minutes before the first attempts were made to take it down. The speech indicates that an expeditious timeframe would be calculated in terms of hours and minutes, rather than days.

Other jurisdictions also have specific laws to deal with fake news, such as Singapore,[73] and revenge porn, such as Japan.[74] While no statute has been enacted in India to deal with a specific online issue, some laws such as the Indecent Representation of Women (Prohibition) Act of 1986 were amended to extend to the online sphere.[75]

Issue specific laws may be a useful way to target problematic content across the internet value chain. But the design of such laws is also an important factor – Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) has received criticism and legal challenge from the opposition Singapore Democratic Party on the grounds that it was used for political censorship.[76]

As seen above, it is possible and even advisable to adopt a variety of mechanisms to deal with the nuances of intermediary liability. Specific laws to target

an issue like fake news have the advantage of being able to tackle misinformation across a variety of media - some that would qualify as intermediaries, like social media platforms, and others like curated online news portals that may not.

Intellectual property rights (IPR) issues

Courts in India treat cases of IPR violations exceptionally and have interpreted the meaning of knowledge differently for copyright infringing content and other unlawful content. The actual knowledge standard for the removal of unlawful content is met when an intermediary receives a notice from a government agency or court order.[77] In the case of IPR violations, however, the aggrieved can approach the platform giving it specific knowledge in the form of specific information about infringing content from the rightsholder.[78]

These different standards of knowledge indicate a more nuanced treatment of the removal of content. They make it clear that intermediaries are not required to actively search for and remove unlawful content (as this would be a huge burden given the sheer volume), but must instead take it down when they receive actual or specific knowledge. Courts have held in subsequent cases that an obligation to proactively find and remove unlawful content cannot be thrust upon intermediaries.[79]

Similarly, the EU Directive on Copyright in the Digital Single Market[80] aims to increase the responsibility of intermediaries for copyright infringing content on their platforms. It has been the subject of some controversy. Article 15 (earlier Article 11) of the Directive, known as the 'link tax', imposes a requirement on news aggregators to pay publishers for using extracts from their articles. Article 17 (earlier Article 13) known as the 'meme ban', requires content sharing service providers to proactively filter copyright infringing content on their platforms. This could take the form of automated filters. These haven't yet come into effect as member states are given a period of two years to process them into domestic law.

The United Kingdom decided not to implement the Directive after its exit from the European Union, citing a desire for greater domestic flexibility in digital regulation.[81] There is also opposition to imposing digital filters in countries such as Germany, where civil society organisations are preparing a legal challenge to the domestic implementation of the Directive which they say results in overbroad censorship.[82]

It is a challenging objective to strike a balance between the concerns of copyright holders and the freedom of expression. It will require an innovative mix of regulation and technology, and cooperation between governments and the large intermediaries. The technological solutions themselves should be goals based. For instance, instead of prescribing a particular method or technology for achieving a certain outcome, regulators can focus on the desired outcome, and incentivise companies to tailor solutions flexibly. Smaller players may also benefit from the trickle down effect of such technology if regulators nudge the most powerful players to innovate and create solutions. An improvement in AI-based filtering for copyright content, for instance, would help fight piracy across platforms.

II.4. Co-Regulatory Model

A co-regulatory approach may help governments achieve the regulatory balance required to foster innovation. In this model, while objectives are set through legislation, the state and private platforms collaborate to attain them. This model also allows other stakeholders to participate and share supervisory power. The diversity of players ensures the constant revision of benchmarks through regular assessment and reviews. It also ensures that public authorities can step in, in case of failure. The EU's regulatory framework acknowledges co-regulation and self-regulation as one of the pillars of their IL regulatory overhaul.[83]

Features of Co-Regulatory Standards

Co-regulatory standards can be characterised by the following:

- **participation and power sharing**
- **multi-level integration**
- **diversity and decentralisation**
- **deliberation among multiple stakeholders**
- **flexibility and revisability**
- **experimentation and knowledge creation[84]**

Box 3

European Parliament's Suggestions for Shaping Digital Regulations

The European Parliament in its report on Reform of the EU Liability Regime for Online Intermediaries released May 2020 suggested some workable measures which may be useful for shaping regulations in the digital landscape. Some of these measures propose that the EU:

- Define the essential public values and establish a multi-stakeholder process for developing commonly agreed regulations, codes of conduct, terms of use and technologies.
- Adopt a vertical approach under which distinct actions would be tailored to diverse wrongdoings, e.g. notice-and-notice[85] for copyright, notice-wait-and-takedown[86] for defamation, and notice-and-takedown and notice-and-suspension[87] for hate speech.
- Incentivise digital entities and users to detect illegality, while minimising the risks and the costs of errors and safeguarding a balance between the different human rights at stake. This can be done by encouraging moderation on a best effort basis, which platforms may avoid at present for fear of being seen as active and consequently losing safe harbour, through a 'Good Samaritan' clause like the one found in 230 CDA.
- Ensure algorithmic transparency so algorithms do not systematically favour any political, ideological or religious opinion, or give preference to content that is their own or produced by an affiliated company.

- **Countries may choose to frame regulations according to the issue, or the type of intermediary.**
- **Some jurisdictions apply the law based on threshold limits for the intermediary.**
- **Co-regulatory models of regulation exclude the disadvantages of self-regulatory and rigid government-controlled models.**

II.5. The Future Indian Imperative

The legal frameworks for intermediaries are in a state of flux. The forthcoming Digital Services Act in the EU will change the established framework of its E-Commerce Directive. Germany and Australia have already imposed greater liability on social media platforms, on the basis of potential harms. Even the USA's 230 CDA, celebrated as 'the twenty-six words that created the internet',[88] has been diluted, as seen with the FOSTA-SESTA package discussed above. India, with its large and untapped market, is in an influential position. It should aim to play a central role in international conversations around setting norms for IL and by exploring workable co-regulatory models. The words of India's future IT laws could shape the internet for years to come.

III. Data Governance

KEY TAKEAWAYS

- A multiplicity of laws governing data can lead to regulatory uncertainty and leave wide scope for judicial interpretation.
- The IT Act is the nodal law governing platforms which collect and process data. Specifying rules for non-personal data under the Act will reduce the scope of regulatory arbitrage by centralising enforcement.
- Data ownership and IPR concerns about the sharing of non-personal data should be settled before a data-sharing framework is designed.
- A framework for data ethics may be key to a trust-based model that doesn't overburden businesses or stifle innovation.
- Transparent cybersecurity regulation is essential for a reliable and secure trust framework of data sharing.

By 2025 it is expected that 463 exabytes of data will be created worldwide each day.[89] Data has evolved from being a by-product of the digital economy to becoming its driver. The fourth industrial revolution is data intensive by design. Moreover, data is considered an infinite and non-rivalrous resource that can be used by several entities simultaneously. These characteristics challenge traditional notions of ownership.

The more the data shared, the more value can be derived from it. Not just the quantity but data quality too determines the value extracted from it. Specifically, in terms of big data, the variety and veracity of data are important ingredients of data quality. Veracity refers to the accuracy of data: at present most of the data collected is unstructured and unreliable. Each year poor data quality costs USD 3.1 trillion to the US economy alone.[90] Variety, on the other hand, is crucial for training AI systems. An absence of variety can lead to issues like algorithmic bias. For instance, research suggests that most facial recognition software has no problem identifying Caucasian males, but may frequently misidentify women of other ethnicities.[91]

The current and future value of data brings its governance to the forefront of the global policy agenda. The tussle between policy objectives like security and privacy is also prominent in the data governance discourse. This chapter assesses the existing data governance framework in India and suggests ways to plug the gaps in it through the IT Act, based on global best practices.

The challenge is to create a governance framework that balances data flows and domestic policy objectives

III.1. Data Governance Challenges

India's data governance relies on a patchwork of conventional legislations that are unable to address new notions of ownership, consent, accountability, agency, etc. However, the discourse on data governance is in a state of flux globally, and centres largely on three basic principles: data ownership and control, protection of personal information, and data flows.

III.1.i Data Ownership and Control

There is no statutory basis of ownership of data under Indian laws. While ownership of datasets or databases is governed by the Copyright Act, there is ambiguity in ownership of the data constituting the database or dataset. The global discourse on data governance is increasingly treating data as property. Like physical property that can only be transferred, sold, licensed, or modified by its rightful owner, identifying the rightful owner of data may be essential to determining the attendant rights attached to it. But ownership rights in physical property are manifest in an either-or binary, whereas the corresponding rights vested in data are layered and difficult to determine. Some of these complexities are discussed below.

Ownership in personal information

The emerging jurisprudence with respect to personal information appears to recognise personal ownership. Property rights in data have led to concerns about balancing data use with adequate protection of individual rights. Further, control over data is often conflated with ownership, a confusion that emanates from data protection legislations, since data protection regimes intend to give data subjects or principals some degree of control over their data. The idea of data ownership, where data subjects/principals are considered owners of their data, may lead to a variety of demands that throw up challenges to data governance.

For example, the concept of individual ownership of personal data may reduce data to a commodity, generating expectations of compensation for its use. A survey of 1,000 respondents in the USA revealed that 79% expected compensation each time their data was used.[92] Conflating control over personal information with ownership may also misinform policymaking or legislation. The idea of full ownership rights to personal data provided the conceptual framework for the Own Your Own Data Act of 2019.[93] The law envisages 'exclusive property right in the data that an individual generates on the internet' and mandates social media platforms to seek licences from users to use their data. It also requires social media platforms to allow users access to information derived from analysis of their personal data. This approach extends the concept of privacy in a manner that may introduce friction in the free flow of information. Conversely, an expression of property rights in data may result in frivolous litigation. It also has the potential to undermine user privacy, as users may trade their private information for little value.[94] India's Personal Data Protection Bill of 2019, in its current form, would not confer the unrestricted right to dispose of one's personal information. It gives data principals limited rights, with exceptions where processing can take place without consent. In cases of non-personal data derived from personal data, the ownership issues are currently being debated.

Ownership as per NPD Committee recommendations

The Kris Gopalakrishnan Committee Report on Non-Personal Data (NPD Report) recommends a regulated framework for access to raw and low to moderately processed data. 95 The report recommends three categories of data based on its source and the entity that collects it: Public non-personal data will be data collected or generated by the governments and considered a national resource. Private non-personal data will be privately owned by the organisations collecting or producing it. And for community non-personal data rights will vest in the data trustee of the concerned community which will benefit from its use. Without going into the specifics of data ownership, the report suggested mandatory sharing of private NPD that pertains to the community. This included raw data to be shared at no remuneration andsome levels of processed data at non-market-based remuneration. Such classifications created a competing interest in data ownership since rights in databases already vest under the Copyright Act. Vide a subsequent report dated December 16, 2020, the committee sought to mitigate this conflict. It recognised proprietary rights in databases, emanating from two sources – copyright and trade secret. In a departure from its initial recommendation, the committee watered down mandatory sharing requirements vis-à-vis databases involving the element of intellectual creativity in its compilation. However, the committee clarified that data sharing can be mandated for certain designated 'high-value data sets'.

It is important to point out that the phrase 'high-value data sets' has not been defined and is thus open to broad interpretation. Therefore, while the updated recommendations try to harmonise non-personal data governance and intellectual property protections, the conflict between the two continues to exist, albeit partially.

Ownership through intellectual property rights

Intellectual property claims in data ownership emanate from copyright or are asserted under confidential information protection mechanisms like trade secrets.[96] Copyright in data is tied to acts of creativity involved in generating data.[97] For example, the copyrightability of databases has been settled by two multilateral treaties, the Berne Convention for the Protection of Literary and Artistic Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights. India has signed and ratified both multilateral treaties.

Computer databases in India are protected as literary works under Section 2(o) of the Copyright Act 1957. Historically, courts recognised the effort expended in compiling facts and protected such compilations to prevent the unjust enrichment of competitors, in what is known as the sweat-of-the-brow doctrine. But in 2007 copyright jurisprudence in India underwent a shift. It now recognises the 'modicum of creativity' doctrine to determine the copyrightability of compilations.[98] The doctrine protects a compilation as an original work, as long as a sufficient level of intellectual creativity and judgment has gone into the creation of that work. The question that still stands is: Will databases compiled through machines enjoy copyright protection?

The application of IPR law to datasets is clear but not so in the case of the data underlying them. Article 2(8) of the Berne Convention provides that the 'protection of this Convention shall not apply to news of the day or to miscellaneous facts having the character of mere items of press information'. This may be interpreted to mean that while some facts are not copyrightable, others may be. The ambiguity is further confounded by Article 10(2) of the TRIPS agreement, which states that:

Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.

While the language of this provision recognises that copyright protection doesn't extend to the data or material constituting a database, it does not foreclose the issue of their copyrightability. Thus, the question around the copyrightability of underlying data in a database, and by extension the question of its ownership, remains unresolved. It is clear however that copyright protection will apply as long as sufficient levels of intellectual creativity were involved in generating the data.

III.1.ii Data Protection

Protecting personal data assumes greater priority in the domestic policy agenda for two broad reasons. First and foremost is the recognition of informational privacy as a fundamental right in the Supreme Court judgment in Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.[99] The second reason is the centrality of personal data to the digital economy, it being the engine that powers recommendation engines, personalisation algorithms and so on.

Even non-personal data derived from personal data runs the risk of re-identification, requiring protection. The NPD Report acknowledges this need and recommends a different treatment for NPD whose underlying data is sensitive or critical personal data. For these reasons, the regulatory framework for NPD must contain provisions to give it adequate protection. Concerns of inadequate protection for NPD are exemplified in the proposed Personal Data Protection Bill. Although a provision in the Bill mandates the sharing of NPD with the Government, neither the Bill nor any other regulatory framework affords protection to such data. As re-identification of data can negate individual privacy, there is a need to harmonise the personal and non-personal data frameworks.

The Risk of De-Anonymisation

Anonymisation tools are not foolproof. Research by the Université Catholique de Louvain and Imperial College London reveals that anonymised datasets can easily be reverse engineered using machine learning to re-identify individuals. The study found that 99.98% of subjects could be correctly re-identified in any available 'anonymised' dataset by using just 15 characteristics, including age, gender, and marital status.[100]

III.1.iii Enabling data flow

A lack of trust between stakeholders (governments, businesses and individuals) impedes the free flow of data within a country and across its borders. Data access and sharing come with risks that range from breach of confidentiality or privacy to violation of public and private interests. Not addressing these concerns through appropriate norms results in the erosion of trust, which impacts the quality of data and introduces friction in its access and free flow.

Data access and sharing at the domestic level

Fostering community trust in the way data is collected, managed, processed, shared and used is critical to the digital economy. A trust deficit impacts individuals as well as businesses and often has cascading effects. An individual concerned about privacy breaches may for instance furnish incorrect information about themself, leading to poor data quality and inaccurate data analytics, ultimately impacting business models too.

A primary concern at the individual level is breaches of privacy and the misuse of personal information. For businesses and other organisations, these concerns pertain to the protection of their commercial interests. For example, the NPD Committee recommended that privately owned non-personal raw data should be shared without remuneration. Notwithstanding the fact that data is non-rivalrous and can be reused, such sweeping provisions may disincentivise investments in data assimilation technologies.

Asymmetries in the protection standards adopted by different organisations may also foster distrust between participants in a data market. For instance, an organisation employing sophisticated data protection standards may not be inclined to share such data with another that does not match those standards, putting smaller businesses at a significant disadvantage.

Cross-border data flows

Policymakers are not confident that domestic policy objectives will be met if citizens' data flows out of their territorial jurisdiction.[101] Concerns of law enforcement, abuse of data, unfair competition, taxation of the digital economy and increased cyberattacks are driving countries to adopt regulatory frameworks that restrict free data flows and access. An estimated 200 data regulations are in force worldwide,[102] and the overall level of restrictiveness by this measure nearly doubled between 2006 and 2016.

Other legitimate sovereign concerns may range from securing hypersensitive data like military or defence information or protecting critical infrastructures like financial systems or energy grids. These exceptions have been recognised under plurilateral trade agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[103] Articles 14.11.3 and 14.13.3 of which identify permissible exceptions for cross-border data flow restrictions, and allow members to adopt data localisation measures to achieve legitimate policy objectives, provided these measures are not unjust, arbitrary or excessive.

III.2. Trust and Data Governance

In light of the concerns discussed above, an environment that facilitates frictionless data flows both domestically and globally can be fostered through mechanisms to enhance trust between governments, businesses, and individuals.

The Osaka Track, a process initiated at the G20 Summit in 2019, aims to expedite efforts in international rulemaking for the digital economy, especially initiatives related to data flows and e-Commerce. The Osaka Leaders' Declaration states that legal framework sboth domestic and international should be respected.

The frameworks must be interoperable to allow data to flow more freely. It thus seeks to strike a balance between sovereignty and global economic interests. It is pertinent to note that India (along with South Africa and Indonesia) refused to sign the Osaka Declaration on Digital Economy. India believes that deliberations pertaining to data governance must be held within the context of the World Trade Organisation.

Box 4

Roadmap for Enabling Cross-border Data Flows

In June 2020 a joint study involving the World Economic Forum, Bahrain Economic Development Board, and a cohort of organisations from around the world developed a roadmap for enabling cross-border data flows.[104] The study identified global best practices and makes six broad recommendations:

1. Allow data to flow by default, by adopting a de-minimis approach to localisation.

2. Establish national frameworks to protect personal information and complement these with laws protecting proprietary rights.

3. Enact a transparent cybersecurity legislation in line with international standards.

4. Establish cooperation mechanisms between national authorities to hold governments accountable for the security and confidentiality of the data they share.

5. Encourage technical standards to increase interoperability, facilitate data portability between businesses, and encourage data publishers to ensure the integrity of data.

6. Future-proof the policy environment by allowing alternative models, such as federated learning models and data trusts, that can fulfil the spirit of cross-border data flows.

Community trust in data is another crucial element that facilitates the use of quality data. An emerging method used to safeguard trust without burdening businesses or stifling innovation through overregulation is through the creation of a data ethics framework: a set of principles guiding the appropriate and responsible use of data. Prominent jurisdictions where such a framework is being explored include the UK[105] and Denmark.[106] Yet the scope of such frameworks varies across jurisdictions, with the UK limiting it to the public sector and Denmark proposing wider applications to include business processes. Key elements constituting such a framework include: maintaining transparency in the use of data, mandating businesses to formulate a data ethics policy, and incentivising data-ethical business models and data sharing practices.

III.3. Enabling Free Data Flows with Trust: Role of the IT Act

Data governance in Indian law is in a state of flux. At present the IT Act is the sole legislation governing data protection and transfer. The proposed PDP Bill and the NPD Committee's recommended governance framework are intended to regulate data flow.

India may consider incorporating good principles of data governance within the IT Act. This may help avoid the unintended consequences of multiple laws governing the same subject matter. As the IT Act is the nodal law governing platforms that collect and process data, specifying principles to govern this process will reduce the scope of regulatory arbitrage. The following table seeks to identify the challenges to frictionless data flows, and suggests solutions based on global best practices.

Box 5

Data Ethics Framework: A Step towards Fostering Trust

Fostering trust goes beyond legally mandated safeguards. Uses for data are expanding at a rapid pace and it is difficult for lawmakers to foresee possible scenarios where data may find application. Moreover, applications of data can have moral and ethical connotations which statutory laws may not be able to address. Consider the Cambridge Analytica scandal, where personal data from millions of Facebook profiles was harvested for commercially motivated political campaigns. While Facebook allows researchers access to user data for academic purposes, it prohibits the use of such data for commercial purposes.[107] Users' consent to collect such data had been obtained only for academic purposes.[108] Even with all reasonable safeguards in place, however, the data was misused.

Another issue, which may not be patently illegal but has moral and ethical implications, is of algorithmic bias. The ramifications of algorithmic biases are particularly severe when they are used in making rights-based determinations. An example is the Risk Assessment Instruments - a class of algorithmic tools designed to predict an individual's future risk of criminal misconduct - used in courts to inform decisions like who can be set free on bail. In the US these tools have been found to exhibit bias against non-White persons. Some assessments revealed that Black Americans were 77% more likely to be pegged as being at higher risk of committing a future violent crime, and 45% more likely to be deemed to commit a future crime of any kind.

Table 6: Suggested Principles for Data Governance

Vertical	Challenge/s	Solution
Technical Interoperability	Collected data is either unstructured or structured in distinctive ways. This makes cross-functional use of data with other datasets difficult. It also deters horizontal use of data across different industries.	Incentivise businesses to adopt similar standards for data, without prescribing a standard. This will allow for a market-based response.
Data Portability	Vendor lock-in, or disincentivising a switch from one vendor to another through prohibitive costs or unfair contractual clauses. In cases like cloud services, vendor lock-in happens due to distinct technical standards and architecture.	Disincentivise or prohibit vendor lock-in practices and promote data portability.
Alternative Data Sharing Models	Innovative data sharing models like federated learning[110] have not been explored.	Create space for businesses to explore such models on fair, reasonable and non-discriminatory terms.
Data Provenance	Data provenance or lineage refers to metadata that records its origin, changes etc. thus protecting the authenticity and integrity of data. The concept has not been recognised or prescribed under the framework.	Encourage the use of technologies like blockchain to record the history of data since it was collected, to ensure authenticity.
Data Ethics	Difficult for lawmakers to foresee possible scenarios where data may find application. Statutory laws may not be able to cater to ethical and moral dimensions of its use.	Mandate a data protection standard that incentivises ethical conduct and data sharing. Use self-certification mechanisms to reduce compliance burden.


BURG
WÄCHTER
Profi

IV. Encryption and Law Enforcement Access

KEY TAKEAWAYS

- Regulations on encryption must balance the rights of privacy and free expression with law enforcement agencies' ability to intercept communications in limited cases.
- One approach is to require technology companies to install backdoors or systemic vulnerabilities, as seen in Australia. It has been criticised as creating larger security risks and may do more harm than good.
- An alternate approach, seen in Germany, is to improve the hacking capabilities of law enforcement. This has made Germany a world leader in encryption technology while meeting the needs of law enforcement access. Yet the use of malware by government agencies has drawn strong opposition from civil rights organisations. The Constitutional Court has held that any surveillance must be within the bounds of the German Basic Law.
- Any balanced framework of interception should ensure adequate checks and balances for oversight, accountability and transparency in the process. The UK's Interception of Communications Code of Practice is an example of such checks and balances.

IV.1. A Modern Problem

Encryption refers to the process of scrambling information such that its contents are accessible only to those with the decryption code or key. Traditionally only governments, militaries, intelligence services or businesses used encryption to protect secrets, but today messaging services such as WhatsApp and Telegram provide secure, end-to-end encrypted platforms for anyone with a smartphone. Several other encryption tools such as the Pretty Good Privacy (PGP) software program are widely accessible and can be used to encrypt data. The Onion Router (Tor) also allows users to encrypt their internet traffic,[111] and virtual private networks (VPNs) can also be used to encrypt internet activity by extending a private network across the public internet.[112]

The emergence of these tools has challenged the ability of law enforcement agencies (LEAs) to monitor and intercept communications in the course of their duties. Encrypted communication services make it hard to detect the spread of misinformation, piracy and illegal content such as child sexual abuse material. Conversely, growing fear of state surveillance particularly after the Snowden revelations in 2013 has led to demands for encrypted communications between individuals.[113]

Encryption has now become a complex debate with implications for privacy, security and product design. Businesses too rely on encryption technologies to safeguard sensitive or valuable information. For instance, B2B cloud service providers (CSPs) that offer data hosting on the cloud often also encrypt the information they store, giving a higher degree of protection to trade secrets, confidential data and even copyright protected materials. Netflix, for instance, uses Transport Layer Security (TLS) which includes encryption to ensure authentication, confidentiality and integrity.[114]

India's IT Act115 empowers government agencies to intercept, monitor and decrypt information.116 The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) Rules 2009 detail the procedures for this. They obligate only the holders of the decryption key to decrypt upon receipt of an order by the competent authority, defined as the Home Secretary at the Union or State level as the case may be. However, subordinate officers are also empowered to do so in certain conditions.

The end-to-end encrypted nature of some communications platforms makes it impossible for agencies to enforce decryption. In most cases encryption is done through protocols where the platform does not have the key, or is implemented by a third party.[117] Consequently there is an impetus to ensure that communications remain traceable via government mandate – as evidenced by the Draft Intermediary Guidelines released in 2019.[118]

The following sections outline various international approaches to the question of law enforcement access. These range from mandating companies to help investigators penetrate their encryption, to building state capacity to do so without weakening encryption protections.

IV.2. The Backdoor Approach

A backdoor is a vulnerability in a system's protection that allows easier access than is otherwise possible. It is a means to access a particular system that circumvents the security measures and mechanisms otherwise built into it. A developer may create a backdoor to enable them to troubleshoot technical problems, or a hacker might install it in a system to compromise it.

LEAs across the world have pushed for access to backdoors to aid investigations. Often they have demanded that companies build these into their products for them. Australia, for instance, passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Act in 2018, compelling companies to assist LEAs with information access - including building new technical tools - upon receipt of a notice from the relevant law enforcement agency.

However, state adversaries can also misuse backdoor vulnerabilities.[119] In the mid-2000s intruders in Greece gained access to telephone switches that were designed to allow interception by LEAs. The intruders monitored and recorded the conversations of over 100 senior government officials including the Prime Minister.[120]

Backdoors can also impair the functionality of the device or product in question. In 2009 Etisalat, the UAE's telecom service provider, installed a US-developed spyware program during a routine update that would send received messages to a central server. Etisalat users suddenly faced crashes, poor reception, reduced battery life, and in some cases their handsets stopped working.[121]

The overall efficacy of the backdoor approach, therefore, is questionable as it deliberately introduces systemic vulnerabilities. In an era of heightened cyberwarfare such vulnerabilities are prone to being used by non-state entities, such as hackers or cybercriminals, or the cyber armies of another state.

IV.3. Other Approaches to Interception

Germany has taken a unique approach to law enforcement access. Rather than weaken encryption through statutory mandates, it builds capabilities for governments to hack into devices, with a legal framework tailored to support such operations. Its 2016 Cybersecurity Policy aims to improve 'security through encryption' and 'security despite encryption'. This policy does not impose limits on encryption, indeed German manufacturers are encouraged to develop encrypted products for national security. It also established a Central Office for Information Technology in the Security Sector (ZITiS) to conduct vulnerability research and to develop and acquire hacking tools and services.[122]

As a result Germany is now a world leader in encryption. While encryption products are protected, the state's use of malware to meet law enforcement objectives has been criticised on grounds of enabling mass surveillance.

The scope of the law, initially limited to international terrorism and risk to life and limb, was broadened to authorise agencies to use hacking as an investigative and intelligence technique for 27 serious crimes. Some of these were crimes against peace, high treason, counterfeiting money or official stamps, and distributing child sexual abuse material. Civil society groups raised questions about the constitutionality of the law, saying it represented an intrusion into privacy and may compromise the integrity of a free and fair press. This led to a court challenge,[123] and in May 2020 the German Federal Constitutional Court deemed the powers unconstitutional in their present form, ruling that the conduct of German security and espionage services must conform with the Grundgesetz (Basic Law or Constitution) even when their operations involve foreigners in a foreign context.[124]

Backdoors exploit vulnerability in the system's protection. This can lead to their misuse.

Germany has not imposed limitations on encryption. It builds state capacity to undertake lawful hacking.

IV.4. Checks and Balances

Checks and balances are essential to ensure there is no misuse of powers of interception and monitoring, as this concerns the privacy and freedom of individuals. In Germany the G-10 law governs all restrictions of the basic right of privacy of correspondence as laid down in Article 10 of the German Constitution.[125] Any interception requires a prior order from the Federal Ministry of the Interior[126] and the approval of a G-10 Commission that includes four members appointed by the parliament, with approval after the fact acceptable in cases of imminent danger.[127] Requiring approval from a non-executive body such as the G-10 Commission of the Parliament is a good way to prevent executive overreach.

The law further entitles people ordinarily to be informed about the surveillance they've been subject to, unless it is undesirable to do so for security reasons.[128] Intelligence agencies are required to answer information requests regarding stored personal data. Annual reports to the parliament are also required.[129] In the UK the Interception of Communications Code of Practice[130] creates similar checks and balances, including dissemination and storage of intercepted information, warrant and application requirements in some cases, and disclosure.[131]

In Australia the Assistance and Access Act mandates that a request or notice must not have the effect of 'requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection' or 'preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection'.132 According to guidance offered by the Australian Department of Home Affairs this means that no company can be compelled to remove a form of electronic protection such as encryption. If the company is not already capable of decrypting something, nothing in the Act can require them to build such capability.133 Additionally, all notices must be reasonable and proportionate, with compliance being practically and technically feasible.

These checks and balances ensure that the extraordinary powers of interception and surveillance are used in a responsible manner keeping in mind the respective rights enshrined in international and domestic law.
On the question of law enforcement access, India too will have to consider the importance of a system of checks and balances. The Puttaswamy judgment[134] held that any restriction on the right to privacy must follow a fourfold test: the action must be sanctioned by law; it must be necessary in a democratic society for a legitimate aim (that does not transgress the fundamental rights); it should pass the test of proportionality (interference in individual privacy must correlate with the threat posed); and there must be procedural guarantees against the abuse of such powers. As seen in Germany's case, oversight by another organ of state such as the legislature or judiciary serves as an important check on government overreach.

It is vital also to harmonise the IT Act with other laws that govern communications interception. For instance Section 5(2) of the Telegraph Act 1885 enables Union and State governments to direct that telegraph messages be intercepted in a public emergency or in the interest of public safety. The procedure is described in Rule 419A of the Telegraph Rules 1951, which state that such directions may be issued by the Union or State Home Secretary. But the rules allow for wide exceptions, where in 'unavoidable circumstances' (a phrase that is given no definition) an officer not below the rank of Joint Secretary may issue such an order. Further, in 'emergent cases' interception can be carried out with the approval of the Head or second-senior-most officer of the authorised law enforcement agency.[135] There is a need to consolidate and harmonise the law relating to interception of communications, including by means outside the IT Act, and create a system of checks and balances which meet the standard set in Puttaswamy.

While the Government has demanded 'traceability' from encrypted apps in the Draft Intermediary Guidelines,[136] it remains unclear if this is in effect a demand to remove encryption. From the international experiences outlined above, introducing backdoors or systemic vulnerabilities into these platforms could potentially destroy the products and endanger all users.

IV.5. The Way Forward

While the Government remains adamant on its demand for traceability, technical methods of doing so without compromising system level encryption should be explored and encouraged. An encryption-friendly approach functions on the understanding that encryption technologies are valuable to individual privacy as well as important tools in securing sensitive commercial information. This perspective moves beyond viewing encryption only as a tool used by bad actors, and instead acknowledges the role encryption can play in countering cyberattacks and enhancing cybersecurity.

In 2015 the Draft National Encryption Policy faced intense backlash for its anti-encryption stance, and consequently MeitY had to issue a clarification exempting products like WhatsApp which are encrypted and have a large user base. Later the Ministry withdrew the draft.[137]

In keeping with the law laid down by the Supreme Court, it is important to focus on a framework of safeguards for the interception of communications by the state. These may be judicial or legislative in nature, to check the executive's use of any powers of interception, ensuring a balance between the objectives of law enforcement agencies and the constitutional rights of the people.

Finally, it is worth exploring India's potential to become a leader in encryption technologies, as Germany has done. Our IT workforce can facilitate this and be a part of India's transformation into a hub of digital innovation in the 21st century.

In Germany, any interception must be approved by a Commission that includes four members appointed by Parliament. People are ordinarily entitled to be informed about the surveillance they've been subject to, unless it is undesirable to so for security reasons. The UK provides for similar checks and balances.

In Australia all notices must be reasonable and proportionate, with compliance being practically and technically feasible.

India must also consider the importance of a system of checks and balances in line with the Puttaswamy judgment.

V. Access and Blocking

KEY TAKEAWAYS

- Section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 form the legal framework governing access blocking in India.
- Website/application blocking is a blunt tool. While it may serve the public interest in certain limited cases, it must be fenced with procedural safeguards.
- The existing provisions in Indian law are broad and are vulnerable to misuse. The number of websites blocked under Section 69A increased from 1,385 in 2017 to 3,635 in 2019.138
- While a statutory framework governing access blocking is desirable, limiting its scope and building in safeguards like due process and transparency provisions are important to prevent misuse.

States around the world restrict access to online content to address a variety of issues. These range from illegal content, like copyright infringing material or child sexual abuse material, to forms of speech and expression deemed improper. Content blocking provisions are usually rooted in law, but despite their legal propriety they are prone to misuse. For example, China uses a spate of regulations to effect nationwide internet censorship and restrict free speech.[139] Provisions for restricting access are overused in India as well: between 2010 and 2018 a total of 14,221 website URLs were blocked in India,[140] and in 2019 alone 3,635 URLs were removed from public access.[141]

V.1. Efficacy of Blocking

The effectiveness of blocking is questionable even for legitimate purposes. This is because blocking access to information may not translate into removal of the illegal content, and most access restrictions are easily skirted. Techniques like IP address-based blocking or URL blocking can be overcome by motivated users, by using a virtual private network or VPN. To illustrate: despite a ban on online pornography in India, traffic data from the leading website PornHub revealed a consistent increase in traffic from India during March-April 2020.[142]

Lack of proportionality is another concern with blocking. Depending on the technique used, content blocking may result in under-blocking, or the over-blocking of lawful content. For example, IP address-based blocking uses barriers like firewalls to block all traffic to an IP address. But a single IP address may host several websites, and such blocking often cuts access to lawful content as well.[143]

While website blocking is a blunt tool, it is not completely ineffective. A 2016 study at Carnegie Mellon University suggested that website blocking led to changes in consumer behaviour, translating into a reduction in piracy. It also indicated that the blocking led to an increase in legal streaming platforms like Netflix.[144]

The following section analyses the legal framework for blocking online content under the IT Act. It also delves into similar provisions in other jurisdictions and seeks to identify global best practices that may be adopted to check its misuse.

The efficacy of blocking is questionable as it is easily skirted and may result in the unintended, disproportionate blocking of legal websites.

V.2. Legal Framework under the IT Act

Section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules of 2009 (Blocking Rules) spell out the legal framework for blocking websites or URLs in India. While the Department of Telecommunications (DoT) may also issue blocking orders to internet service providers to enforce licensing conditions, they are not the subject matter of this report.

Section 69A is an overbroad provision which allows the Union government to block any information 'generated, transmitted, received, stored or hosted' in any computer, if it is satisfied with the necessity and expediency of such action in the interest of the:

- Sovereignty and integrity of India
- Defence of India
- Security of the state
- Friendly relations with foreign states
- Public order
- Preventing incitement to the commission of any cognisable offence relating to above.

Orders issued under 69A are binding and violation is penalised by imprisonment up to seven years and a fine.[145] The Blocking Rules detail the procedures that need to be followed before a blocking order is issued.

In ordinary circumstances, each blocking request must be placed before a Committee for Examination of Request,[146] which must assess whether the request meets the criteria listed above and issue its recommendation after allowing the person or intermediary hosting such content a chance to represent themselves. Based on the committee's recommendations the Secretary of MeiTY may issue an approval pursuant to which an order is issued. Although the intermediary is given at least 48 hours to prepare for the hearing, the Rules do not prescribe a time limit within which the intermediary must be heard.

The Blocking Rules also provide for conditions of 'emergency nature'[147] in which the ordinary procedure may be bypassed. MeitY recently banned over 200 applications including TikTok and WeChat under these emergency powers. In such situations the order to block is issued before the matter is placed before the Committee for Examination of Request, and the intermediary is not given the opportunity to be heard. They may appear before the Committee only after the request to block has been brought before it, which cannot be later than 48 hours after the direction to block. Given that the Rules do not define 'emergency nature', and that the checks and balances for the ordinary procedure are available only after the blocking has comeinto effect, they leave scope for arbitrary decision making.

The Rules also require that strict confidentiality be maintained about the complaint and action taken.[148] As a result the blocking order is often not communicated to the intermediary and is not made public. While the provision may not be unconstitutional, in practice its vague and wide sweep is debatable.

Under the IT Act, blocking is done under strict confidentiality and on broad grounds.

Blocking can be imposed under circumstances of 'emergency nature' but the term is not defined.

V.3. Alignment with International Conventions

V.3.i International Principles on Free Speech

The United Nations Office of the Commissioner of Human Rights has interpreted Article 19(1) of the International Covenant on Civil and Political Rights (ICCPR) to mean that modes of expression protected under the article include 'all forms of audio visual electronic and Internet based modes of expression'.[149] According to its recommendations, restrictions on access to information are permissible only if they are content specific, not generic, and are not prohibited solely because the content is critical of the government or the political social system espoused by the government.

Similarly the 2011 Joint Declaration on Freedom of Expression recommended tailored approaches for responding to illegal content online.

Box 6

Validity of Section 69A: Ground Reality

The constitutional validity of Section 69A was called into question in Shreya Singhal v. Union of India but the Supreme Court upheld its validity stating that it had several safeguards. First, blocking can only be resorted to where the Union government is satisfied that it is necessary to do so. Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). Third, reasons must be recorded in writing in such a blocking order so they may be assailed in a writ petition under Article 226 of the Constitution.

In practice, however, the implementation of these Rules leaves much to be desired. Due to the confidentiality clause under Rule 16 no information about the complaints and action taken is made public. This makes it difficult to discover whether an inaccessible website has been blocked, why that has happened, and whether the procedures under the Rules were followed.

The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression in its 2011 report emphasised that the wide powers vested in governments to block websites contravene the ICCPR.[150] The Rapporteur gave four main reasons for this. First, the conditions that justify blocking are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Second, blocking is not justified in pursuit of aims listed in Article 19 of the ICCPR,[151] and blocking lists are generally kept secret, making it difficult to assess whether access to content is being restricted for a legitimate purpose.

Third, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that deemed illegal. Fourth, content is frequently blocked without the intervention of or possibility of review by a judicial or independent body.

Box 7

Test for Restriction of Content on the Internet according to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Restrictions imposed as an exceptional measure on online content must pass a three-part cumulative test:

a) Blocking or filtering provisions should be clearly provided by law which is clear and accessible to everyone;
b) Blocking orders must be strictly in line with the requirements of Article 19(3) of the International Covenant on Civil and Political Rights;[152]
c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

The rapporteur recommended additionally that

- Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body independent of any political, commercial or other unwarranted influences.
- National law should be sufficiently precise, with sufficient safeguards against abuse or misuse to prevent any 'mission creep' including in oversight.
- There should be review by an independent and impartial tribunal or regulatory body.
- There should also be adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.

V.3.ii International Trade Law

On 26 April 2020 the Dispute Settlement Body (DSB) of the WTO adopted a Panel ruling to clarify the use of national security exceptions to WTO rules as invoked in the dispute between Russian and Ukraine over transit restrictions.[153] Specifically, the Panel held that invocation of the national security exception is justiciable and subject to scrutiny by the WTO's DSB. The decision came against the backdrop of the USA's long held position that the exception is totally 'self-judging', i.e. that it can be unilaterally invoked by a Member without the possibility of further scrutiny.

Traditionally used as an instrument to control investments in strategic sectors like the military, the scope of national security considerations to scrutinise the participation of private players in strategic and critical sectors has evolved significantly. For instance, in three separate press releases the MeitY banned more than 150 Chinese-origin applications on the assertion that these applications were involved in activities detrimental to the sovereignty and security of India.[154]

In the event that India's action is challenged before the WTO, it is likely to argue that the ban was necessary to protect its essential security interests taken in time of war or any other international relations emergency. This phrase was recently interpreted by a WTO Panel in the Saudi Arabia/Qatar decision (2020).[155] Based on the Panel's analysis, India will have to demonstrate that three conditions were fulfilled: there was a situation of 'war or other emergency in international relations'; such a ban was adopted during such war or emergency; and the ban was not remote or unrelated and was a plausible measure to protect India's essential security interests.

The term 'emergency in international relations' has been interpreted by the WTO to mean a situation of armed conflict, or latent armed conflict, or heightened tension or crisis, or general instability engulfing or surrounding a state.

Based on the above precedents, India will have to prove that the ban on Chinese applications was not remote or unrelated to the Indo-China border clash, and was necessary to protect Indian territory or population from external threats. It is worth noting that the relevant MeiTY press release does not explain how each banned app is a threat to India's essential security interests, instead announcing a blanket ban for all apps. These apps vary widely in the nature of the services they provide, and include e-Commerce apps, news aggregators, web browsers, utility apps and social media apps. Therefore, the types of user data they collect would also vary widely. India moreover does not have a domestic law that prohibits user data from being transferred outside its territory. Therefore, there is nothing illegal or unauthorised per se in transferring data to servers located outside India. As observed in the WTO's Russia/Ukraine and Saudi/Qatar

Box 8

WTO and National Security

The global trading framework under the aegis of the World Trade Organisation is guided by two key principles: the Most Favoured Nation principle, which restricts member states from discriminating between trading partners, and National Treatment principles that require member states to treat foreigners and locals alike. The national security exception available in WTO agreements purportedly allows members to breach their obligations. Specifically, it allows states to adopt measures to protect their 'essential security interest'.

Pertinently, the agreements provide that actions for essential security interest must relate to: fissionable materials or the materials from which they are derived; the traffic in arms, ammunition, and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly to supply a military establishment; and must be taken in time of war or other emergency in international relations. The WTO's adjudicatory body has interpreted the term 'war or other emergency in international relations' to mean a situation of armed conflict, or latent armed conflict, or heightened tension or crisis, or general instability engulfing or surrounding a state.

decisions, a WTO Panel will require India to provide factual evidence proving why each banned app is a threat to its essential security interest.

V.4. Position in Other Jurisdictions

There are broadly speaking two prevalent models for regulating the blocking of online content:

General legal provisions such as in Estonia, Iceland, Canada where there is no specific legislation governing the blocking of online content. These jurisdictions extend general legal provisions to cover online content.

Specific legal provisions such as in India, Brazil, Singapore where the blocking or filtering of online content is governed by a specific legislation.

States that follow the first model also rank highly on Freedom House's Freedom on the Net ranking as compared with states that follow the second.[156] While one may expect a defined legal framework to restrict the discretionary element within the confines of due process, and lend predictability to regulatory action, there are examples of statutory provisions being broadly interpreted by courts and regulators, giving them unintended effects.

For example in December 2015 a Brazilian court passed an order to ban WhatsApp using a clause under Article 12 of the Marco Civil Da Internet, a law widely celebrated as the model for rights-based internet governance. The article, which provides for penalising companies that violate data protection norms under the law, was improperly used to penalise WhatsApp for not complying with a request for user information.[157]

While a codified legal framework for the blocking or filtering of content may be desirable, it is imperative that the law is not vulnerable to misuse. This may be achieved by scope limitation and building safeguards within legal provisions.

An example of scope limitation is Section 23 of the UK's Digital Economy Act 2017, which provides for blocking access but is limited either to extreme pornographic content or pornographic content provided to a minor. In terms of safeguards, the test laid down by the English Court of Appeal in *Cartier International AG v. British Sky Broadcasting Ltd* may serve as good guidance.[158] The court, while upholding a website blocking order in a case concerning the infringement of intellectual property rights, endorsed the following principles or factors as relevant in determining if a site-blocking order is proportional:

Necessity or a consideration of the extent to which the relief is necessary to protect the plaintiff's rights. The relief need not be indispensable, but the court may consider whether alternative and less onerous measures are available.

Effectiveness or a consideration whether the relief sought will make infringing activities more difficult to achieve and discourage internet users from accessing the infringing service.

Dissuasiveness or a consideration whether others not currently accessing the infringing service will be dissuaded from doing so.

Complexity and cost or a consideration of the complexity and cost of implementing the relief sought.

Barriers to legitimate use or trade, a consideration whether the relief will create barriers to legitimate use by unduly affecting the ability of users of ISP services to access information lawfully.

Fairness or a consideration whether the relief strikes a fair balance between fundamental rights of the parties, the third parties, and the general public.

Substitution or a consideration of the extent to which blocked websites may be replaced or substituted, and whether a blocked website may be substituted for another infringing website, and

Safeguards or a consideration of whether the relief sought includes measures that safeguard against abuse.

This test was recently referenced and adopted by the Canadian Federal Court in the case of *Bell Media Inc. v GoldTV.biz*.[159]

A codified legal framework for blocking should have adequate safeguards to prevent its misuse

V.5. The Way Forward

The blocking provisions under the IT Act merit revision. It is critical to hardwire checks and balances in the law through enhanced accountability and transparency mechanisms. In this backdrop, provisions like Rule 16 of the Blocking Rules, which mandates strict confidentiality regarding blocking requests, need particular reconsideration. Additionally, blocking provisions should be used sparingly, temporarily and within the confines of a just, fair, and reasonable procedure. Adherence to such safeguards will help maintain the Act's consonance with global best practices, both in terms of free speech and free trade.

Box 9

Policy Recommendations for Blocking

The Internet Society[160] and Freedom House[161] have given recommendations to minimise the negative effects of blocking. These include:

- Last resort – Blocking orders should be used sparingly, and only as the last resort. All non-blocking options must be exhausted before restricting access to a website/URL.
- Maintain transparency – Blocked content and the underlying reason for such blocking must be disclosed to the public. Regulators should also ensure that the persons concerned have an avenue to voice their concerns.
- Blocking should be temporary – Blocking measures must be temporary and should cease to apply once the reason for such blocking ceases to exist.
- Involve stakeholders – The development and implementation of policy governing the blocking of online content should be informed by all stakeholders, including experts in matters of technology, economy, the arts, and consumer rights.
- Due process – Procedures governing the blocking of online content must be just and fair. The authority should ensure that the affected party is afforded a chance to be heard before an order is passed. The procedure should provide for checks and balances like independent review and appeal to ensure procedural fairness.

VI. Cybersecurity

KEY TAKEAWAYS

- The definition of cybersecurity in the IT Act is over a decade old. It was designed for a homogeneous devices ecosystem and is inadequate to cover the full spectrum of devices in the Internet of Things. It merits revision in the light of the expanding cybersecurity threat.
- The definition of cybersecurity is non-compliant with the Confidentiality Integrity Availability triad, the gold standard for information security. While it covers the confidentiality and integrity aspects, the availability aspect is not clearly expressed.
- The penal compensatory damages provided under Section 43 are inadequate compared to global standards and lack deterrent power. The section also precludes prosecution for offences involving the misuse of authorised access.
- Protecting critical information infrastructure is a shared responsibility between the public and private sector. However, the administrative structure of the NCIIPC is not suited to multi-stakeholder functioning.

The National Crime Records Bureau reports that cybercrime incidents in India more than doubled from 2016 to 2018, from 12,137 to 27,248.[162] In 2019 India was among the five most cyber attacked countries in the world.[163] Most of these attacks were aimed at the country's critical information infrastructure: computer resources critical to national security, economy, public health or safety. The risk of a cyber attack looms large over individuals, businesses and governments. The World Economic Forum's Global Risk Report 2020 names them among the top ten prevailing global risks in terms of likelihood and impact.[164] Research suggests that three out of five businesses in the Asia-Pacific region are putting off digitisation from fear of cyber attacks.[165] Ensuring a safe cyberspace is thus essential to drive growth in the digital economy.

A safe and secure cyberspace is the shared responsibility of all countries that constitute the global internet. Individual users and organisations may use two-factor authentication or encryption to protect their assets. States may protect cyberspace by criminalising conduct that jeopardises their security or integrity, or by mandating organisations to implement security measures that protect critical infrastructure.

In India the IT Act is the statutory instrument of state action to ensure cybersecurity. It relies on two remedies: criminalising certain cyber activities, and creating an organisational framework to address cybersecurity issues in critical and non-critical sectors.

These cybersecurity provisions were introduced in 2008 and haven't been amended since. Meanwhile, cyberspace has graduated from the personal computer era where threats were limited to viruses and worms, to the Social, Mobile, Analytics and Cloud or SMAC era. Advanced persistent threats, or cyberattacks carried out over extended periods to steal valuable data, are the principal concern. Machine learning and artificial intelligence are the next frontiers that malicious actors intend to conquer. For example in 2018 IBM's

Cyber Security Intelligence team unveiled DeepLocker, an AI-modelled malware capable of remaining undetected until it reaches its target.

India's legal framework for ensuring cybersecurity is ill equipped to tackle existing or future challenges. This chapter analyses the cybersecurity framework of the IT Act in comparison with global best practices, to identify specific areas that merit re-examination. It analyses offences under the Act to highlight gaps in the current approach, and considers the functional aspects of the organisational framework created under the Act to assess its efficacy.

VI.1. Cybersecurity under the IT Act

The IT Act and associated rules and regulations are the bedrock of India's cybersecurity architecture. Although each sector has its own set of guidelines to supplement this framework, they are not the subject of this report.

VI.1.i Legal Framework

Definitional Issues

The definition of cybersecurity in the IT Act is critical because it determines the scope of other provisions that rely on it. Section 70B(4) of the IT Act for instance describes the functions of the Indian Computer Emergency Response Team or CERT-In, the nodal agency for any cyber incident response in India. The section says these are to be performed 'in the area of cyber security', thus the scope of CERT-In's functions will be proportional to the scope of the definition of cybersecurity.

As defined in Section 2(1)(nb) of the IT Act, cybersecurity is the act of

Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification, or destruction.

This definition is not in sync with prevalent global security standards. In fact it does not cover the minimum standard of protection represented in information security parlance as the 'CIA triad'.

This triad is a globally accepted security model designed to guide information security policies and legislation on cybercrimes and cybersecurity. It breaks down information security into three essential components: confidentiality (information should not be disclosed to unauthorised persons), integrity (data should not be modified without authorisation) and availability (the guarantee that reliable information will be available to authorized users when needed).

The International Telecommunication Union's 2018 Guide to Developing a National Cybersecurity Strategy also prescribes that legislations and regulations should be aimed at preventing, combating and mitigating actions directed against the confidentiality, integrity and availability of ICT systems and infrastructures.[166]

The definition of cybersecurity in the IT Act fails to capture distinctly the three elements of the CIA triad - particularly the principle of availability. It seeks to protect a computer or the information within it from unauthorised access, use or disclosure (maintaining confidentiality) or from disruption, modification or

destruction (maintaining integrity). It does not define the availability of reliable information as a lynchpin.

Other jurisdictions by contrast define cybersecurity to clearly delineate the three aspects of the CIA triad. Singapore's Cybersecurity Act 2018 for instance defines it as:

the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state –

a. the computer or computer system continues to be available and operational;

b. the integrity of the computer or computer system is maintained;

c. and the integrity and confidentiality of information stored in, processed by, or transmitted through the computer or computer system is maintained.

A clear demarcation between the three elements of confidentiality, integrity and availability is visible in other domestic rules and regulations. The Reserve Bank of India's Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds 2011[167] recognise the triad as the core of its information security strategy. Similarly the Securities and Exchange Board of India's Cyber Security and Cyber Resilience Framework of Stock Exchanges, Clearing Corporation and Depositories prescribes the globally accepted NIST (National Institute of Standards and Technology) cybersecurity framework,[168] which is built on top of the CIA triad. Hence, expanding the scope of the definition of cybersecurity under the Act to clearly incorporate all three elements of the triad will bridge the dissonance between the statute and sectoral guidelines.

Another deficiency is the ambiguity in covering the full spectrum of Internet of Things (IoT) devices within the definition of cybersecurity. Estimates suggest that there are more than 21 billion IoT devices in the world today with the number expected to double by 2025.[169] These devices are vulnerable to security breaches and can also be used as vectors to cause large scale cyber attacks. In 2020 more than 25% of identified enterprise level cyber attacks were expected to involve IoT devices.[170]

Box 10

Exploiting IoT Vulnerabilities: The Mirai Botnet Attack

In 2016 a malware called 'Mirai' used common default credentials (such as a username and password being set by the manufacturer as 'admin') and poor configuration of connected devices to create a botnet army to launch a Distributed Denial of Service attack. The attack impacted multiple services including French cloud computing company OVH and internet services company Dyn, ultimately causing temporary outages of platforms like Netflix, GitHub and Twitter.

Unlike conventional information technology devices, IoT devices, given the variety of physical environments they may be used in, are vulnerable to tampering.[171],[172] IoT devices also sometimes lack the computing power of a conventional device, making it difficult to implement standard security practices like encryption. The operational requirements for resilience and security in an IoT device differ from common cybersecurity and privacy practices for conventional devices.[173] Consequently many IoT devices do not fit the definitions of standard information technology devices.[174]

Given this backdrop the 12 year old definition in the IT Act, designed to cover conventional devices, may not cover the full spectrum of IoT devices. The Act limits cybersecurity to computer, computer resource and communication devices. It defines these terms to include data processing devices which perform logical, arithmetic, memory or communications functions. This may exclude simpler IoT devices like connected thermostats, which do not perform such functions but are nevertheless connected to the internet.

Globally, jurisdictions have tackled the issue of IoT cybersecurity through separate and specific instruments ranging from statutory amendments, as in the case of California,[175] to codes of practice implemented by the UK,[176] Australia[177] and Singapore.[178]

VI.1.ii Comparison with other jurisdictions

The approach of criminalising cyber misconduct with graded penalties is found in many jurisdictions. The UK's Computer Misuse Act 1990, Singapore's Computer Misuse Act 1993, and the USA's Computer Fraud and Abuse Act adopt a similar approach. India's IT Act too specifies graded penalties for such offences, as listed below.

Box 11

California's IoT Security Law

This legislation uses the term 'connected device' as a broad term to include the entire spectrum of IoT devices. It defines a connected device as 'any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.'

The definition of cybersecurity under the IT Act is not fully compliant with the CIA triad, the basic minimum standard of information security.

Coverage of the full spectrum of the IoT ecosystem under the definition remains ambiguous.

Box 12

Graded Penalties in the IT Act

India penalises actions that may adversely impact the confidentiality, integrity and accessibility of networks and devices. These may be classified into the following categories:

a. Simple form – Here the motive is immaterial and the mere act is punishable. Such offences include hacking, denial of service attacks, and contamination, punishable under Section 43. The penalty is to compensate the affected party.

b. Aggravated form – The offences defined under Section 43, if committed with dishonest or fraudulent intent, are punishable under Section 66. A convicted person can be imprisoned for up to three years, or pay a fine up to Rs 5 lakhs or both.

c. Cyber terrorism – A person found guilty of committing similar offences, with the intent of threatening the unity, integrity, security or sovereignty of India, or to strike terror in the people or any section of the people, is punishable under Section 66F. The maximum punishment is life imprisonment.

Despite the similarities, India's approach diverges from these jurisdictions in the following ways:

No distinction between lack of authorization and exceeding authorization

Section 43 of the IT Act penalises unauthorised access. The offence is based on the assumption that the person committing it was not authorised to access the affected computer or network. But it does not cover cases where an authorised person exceeds their authorisation to commit an offence.

In 2005 an Expert Committee formed to recommend changes to the IT Act suggested that the phrase 'without the permission of the owner' in Section 43 should include access to information that exceeds the level of authorised permission to access. But the recommendation was overlooked in the amendment Act.[179]

In other jurisdictions, provisions against exceeding authorisation are either statutorily embedded, as in the US Computer Fraud and Abuse Act, or have been given effect through judicial interpretation as in the United Kingdom, where the concept was introduced by the House of Lords in *Regina v. Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America.*[180] The judgment overturned the decision in *Director of Public Prosecution v. Bignell and Another* to introduce the concept of unauthorised use of authorised access.[181]

In the Bignell case, two police officers instructed computer operators to access the Police National Computer (PNC) for private, unofficial purposes despite knowing the PNC was only to be accessed for official purposes. The officers were convicted by the stipendiary magistrate for the offence of unauthorised access under Section 1 of the Computer Misuse Act of 1990. However, on appeal the Divisional Court held that an offence of unauthorised access could be made against the accused officers as they were authorised to access the PNC. This interpretation remained the law of the land for two years. In 1999 while deciding Regina v. Bow the House of Lords overturned Bignell to recognise exceeding authorization as an offence under the Computer Misuse Act.

Box 13

Exploiting IoT Vulnerabilities: The Mirai Botnet Attack

In 2016 a malware called 'Mirai' used common default credentials (such as a username and password being set by the manufacturer as 'admin') and poor configuration of connected devices to create a botnet army to launch a Distributed Denial of Service attack. The attack impacted multiple services including French cloud computing company OVH and internet services company Dyn, ultimately causing temporary outages of platforms like Netflix, GitHub and Twitter.

Inadequate deterrence

Section 43 imposes a penalty in the form of compensation to affected parties, but it does not specify the quantum of compensation nor lays down the principles that may guide its determination.

Regulatory frameworks in other jurisdictions provide for stricter punishment. Section 1 of the UK's Computer Misuse Act stipulates imprisonment ranging from 12 months to two years or a fine or both. Similarly, Singapore's Computer Misuse Act 1993 stipulates imprisonment up to two years and a fine up to 5,000 dollars on the first conviction. On subsequent conviction imprisonment may go up to three years and the fine up to 10,000 dollars.

By contrast the penalties under the IT Act are inadequate and lack deterrent power. The offences defined under Section 43 are capable of inflicting serious damage to networks and devices which may not always be quantifiable in monetary terms. For example, cryptojacking or the illicit use of a victim's computingpower to mine cryptocurrencies, may not damage the infected device, but it will slow down processes that may result in a loss of productivity, which are hard to justify in a court of law.

Moreover, compensatory penalties, especially when not quantified, leave scope for arbitrary determination by the judiciary. While stricter sanctions are advisable, the requisite safeguards must be in place to protect ethical hackers involved in penetration testing or researchers working towards gathering threat intelligence. Similar discussions are already underway in other jurisdictions. In the UK the Criminal Law Reform Now Network in its 2020 report titled Reforming the Computer Misuse Act[182] highlighted protection for ethical hackers and academicians as a priority area.

Box 14

Why Penalties are Minimal in Section 43

It is important to understand the reason Section 43 prescribes minimal penalties. The IT Act in its original form provided for limited offences: hacking, tampering with computer source codes, or electronically sharing 'obscene' content. Each of these offences was punishable with imprisonment or a monetary fine. Later the Expert Committee charged with suggesting changes to the Act recommended reducing such penalties, because 'sometimes, because of lack of knowledge or for curiosity, new learners / Netizens unintentionally or without knowing that it is not correct to do so, end up doing certain undesirable acts on the Net'.[183] The quantum of penalty was thus deliberately reduced so as not to deter users from adopting new technology. This rationale is not relevant in the present era and thus the provision warrants reconsideration, with sufficient safeguards for ethical hackers.

Limited scope of the threshold of intention

Compared to Section 43, Section 66 lays down stricter punishments for offences committed with dishonest or fraudulent intent. However the threshold of dishonest or fraudulent intent is misplaced for cyber offences as it limits the application of Section 66. The terms dishonestly and fraudulently as used in the Act import their definitions from the Indian Penal Code of 1860 (IPC) which defines them as:

- **Dishonestly** – Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing dishonestly.

- **Fraudulently** – A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

The terms 'wrongful gain' and 'wrongful loss' in the definition of dishonestly are defined in Section 23 of the IPC to mean unlawful gain or loss of property. Thus, dishonest intent is tied to the conception of corporeal property and ownership. To subject offences defined under Section 43 to the threshold of fraudulent intention would limit them to cases concerning financial injury.

In effect Section 66 fails to recognise other forms of intent, like the intent to cause bodily harm. This is a glaring omission because of the exponential growth expected in the Internet of Medical Things market. IoMT is a variation of IoT, where connected medical devices and software are leveraged to capture patient data in real time, to help improve the speed and accuracy of diagnosis and treatment. IoMT devices include wearable external devices like insulin pumps, and their implantable counterparts such as pacemakers and neurostimulators. Pacemakers are susceptible to life-threatening security vulnerabilities that could be exploited to remotely control the implanted device.

Other jurisdictions do not use such a limited threshold of intention. In the UK and Singapore, the threshold of intent is tied to committing or facilitating the commission of further offences. Singapore's Computer Misuse Act 1993 clarifies these offences to include those involving property, fraud, dishonesty or bodily harm. The UK's Computer Misuse Act 1990 has an even wider scope, covering any offence for which the law provides a penalty.

Grading penalties based on the quantum or nature of damage caused by an offence may be a better model. For example, in France the punishment for fraudulent access is imprisonment and a fine of up to €60,000 under Article 323-I of the French Penal Code, which concerns unauthorised access to an automated data processing system. When data is modified or suppressed as a result of unauthorised access, the sanction is three years' imprisonment and a fine up to €100,000. For offences committed in a public or governmental system, the sanction is raised to five years' imprisonment and a fine up to €150,000.

In addition to penalising unauthorised access, the IT Act should account for offences committed by exceeding authorised access.

When a compensatory penalty is not quantified it leaves scope for arbitrary determination by the judiciary.

Section 66 fails to recognise forms of intent other than dishonest or fraudulent intent.

India could consider grading penalties based on the quantum or nature of damage caused by an action.

VI.2. Organisational Framework

The Information Technology (Amendment) Act 2008 introduced two new sections, 70A and 70B, to create an organisational framework to address cybersecurity challenges for critical and non-critical infrastructure. Consequently the following bodies were set up: the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In) including sectoral CERTs.

Other government agencies involved in cybersecurity operate outside the ambit of the IT Act. These include the Cyber and Information Security Division and the Indian Cyber Crime Coordination Centre under the Union Ministry of Home Affairs, and the National Cyber Security Coordinator under the Prime Minister's Office. These agencies are beyond the scope of this report.

Box 15

National Critical Information Infrastructure Protection Centre (NCIIPC) – Designated as the national nodal agency to protect critical infrastructure under Section 70A of the IT Act, it functions under the administrative control of the National Te hnical Research Organisation, a technical intelligence agency governed by the National Security Advisor.

Indian Computer Emergency Response Team (CERT-In) – Created under Section 70B of the IT Act, CERT-In is tasked with forecasting and responding to cyber attacks, and issuing advisories on security practices. The establishment of sectoral CERTs, especially for critical sectors, is also under consideration. CERT Thermal, CERT Hydro, CERT Transmission and CERT Distribution are already functional in the power sector. Proposals for sectoral CERTs were also mooted for the financial and telecom sector.

Fragmented cybersecurity framework

India is one of the few states with a decentralised cybersecurity framework. There is a dearth of research on the efficacy of this model, but the ITU's Global Cybersecurity Index (GCI) can be relied on to identify the preferred practice in this regard.[184]

The GCI is a composite index combining 25 indicators to monitor and compare the cybersecurity commitment of states relative to the five pillars of the ITU's Global Cybersecurity Agenda. One of these pillars is organisational measures, which evaluates the presence of institutions and strategies for developing cybersecurity measures nationally. The UK, USA and France are the top three performing jurisdictions on the index. They also score highest on the organisational metric. They rely on a single cybersecurity agency to oversee critical as well as non-critical infrastructure. This trend is also visible in Estonia, Canada, Malaysia and Singapore - jurisdictions that also rank high on the organisational metric.

The performance of these jurisdictions suggests that a single nodal agency covering all aspects of cybersecurity may be more effective. Responses to cyberattacks are time sensitive and the existence of separate agencies creates an additional layer of coordination which may delay response time and may prove counterpro ductive. In this backdrop, the Indian model has been criticised

Absence of shared responsibility

The security of cyberspace relies also on a state's ability to leverage the expertise of industry and academia. Public-private collaboration to protect critical infrastructure is one of the key pillars of the layered cyber deterrence strategy recommended by the United States Cyberspace Solarium Commission established by the US Congress in 2019. In its report of March 2020 the commission emphasised that, unlike in the physical domain, the government is not a primary actor in cyberspace. It stated, 'If the U.S. government cannot find a way to seamlessly collaborate with the private sector to build a resilient cyber ecosystem, the nation will never be secure.'

In this regard the UK's National Cyber Security Centre implements a workable model. The NCSC identifies the use of industry and academic expertise as one of its core goals and has designed specific programs to this effect. Similar efforts have been made by Singapore's Cyber Security Agency.

Box 16

Collaborative Approach to Cyber Security

Industry 100 is the UK's National Cyber Security Center's principal initiative to facilitate collaboration between the agency and industry.[185] It allows selected industry members to take up temporary roles within the NCSC, facilitating cross-sectoral learning.

Similarly, Singapore's Cyber Security Agency runs the SG Cyber Talent Initiative, which aims to develop a cybersecurity workforce through collaboration with industry and academia. Activities planned under the initiative for the year 2020 includes the SG Cyber Olympics, which involves identifying talents and training them in advanced cybersecurity.

India by contrast does not emphasise collaborations with industry or academia. While the composition of CERT-In's Advisory Committee mandates the representation of industry associations and academia, it limits the scope of their participation to one member from each field. Academic representation is limited to the Indian Institute of Science. Similarly, while the NCIIPC's advisory council mandates representation from industry, the fact that it functions under an intelligence agency limits the scope of industry collaboration.[186] This is problematic because the protection of critical information infrastructure is a shared responsibility in which the private sector has a major role to play.

A single nodal agency that covers all aspects of cybersecurity may be more effective than a fragmented and uncoordinated model.

Protecting critical information infrastructure is a shared responsibility in which the private sector has a major role to play.

VI.3. The Way Forward

Legal provisions relating to cybersecurity were introduced in 2008 and have not been updated since, even as the nature of threats in cyberspace becomes increasingly complex and sophisticated. To create a future-proof legal framework, the IT Act will have to adopt a technology agnostic definition of cybersecurity. It must also provide for more stringent penalties in order to have a deterrent effect.

There is merit in revisiting the organisational framework overseeing India's cybersecurity challenges. International experience indicates that a centralised framework helmed by a single agency is effective. Cybersecurity is a joint imperative, served best by a multi-stakeholder approach. Thus the framework must also facilitate closer cooperation with non-government stakeholders including industry and academia.

Summary of Recommendations

Chapter I – e-Commerce

Need a consistent definition of the term electronic commerce – Though the IT Act was passed with the intent to facilitate e-Commerce it does not define the term. This lacuna affords various regulators and authorities the luxury to create distinct definitions of the term to suit their needs, creating uncertainties and inconsistencies in the application of the law to various e-Commerce entities.

Jurisdictional boundaries of government regulators and supervisors should be clarified – According to the existing allocation rules, multiple government departments including the Department for Promotion of Industry and Internal Trade, Ministry of Electronics and Information Technology, and the Department of Telecommunications have been vested with rulemaking powers to govern digital businesses. The consequence of ambiguous jurisdictional boundaries is that several government arms can frame their own regulations. The result has been disputes over supervisory roles and confusion among market players over the applicability of legal instruments.

India should consider a vertical approach to regulation that can improve efficiency in the policymaking process – A vertical approach to regulation can aid in healthy division of work, with each level of government doing what it does best. It would empower sectoral regulators to create rules affecting only those within their regulatory remit, with principal legislation such as the IT Act to provide overarching legal certainty.

Chapter II – Intermediary Liability

Clear demarcation of different types of intermediaries – The IT Act follows a one size fits all approach to regulating intermediaries. The expansive definition of an intermediary in the Act covers everything from social media platforms to internet service providers (ISPs) and cyber cafes. However, intermediaries are heterogeneous and often have varying degrees of control over the content transmitted through them. Hence, clear demarcation of the various types of intermediaries is important for effective rulemaking.

Need for greater accountability – The safe harbour approach to determining intermediary liability allowed platforms to attain scale. It also led to unanticipated economic, social, and political disruptions like the spread of misinformation, online piracy, and the circulation of child sexual abuse material and terrorist recruitment material. Several countries have introduced liabilities based on the types of platform, their thresholds, and specific issues such as fake news or revenge porn. India must follow suit to explore regulatory models that allow greater accountability without imposing stifling regulations.

A co-regulatory approach may be explored – A co-regulatory approach can help the government achieve the regulatory balance required to foster innovation. Under this model, while the objectives are set through legislation, the state and private entities collaborate to attain them. The model also allows other stakeholders to participate and share supervisory power. The diversity of players ensures a constant revision of benchmarks through regular assessment and reviews. At the same time it ensures that public authorities can step in, in case of failure.

Chapter III – Data Governance

Create a legal framework enabling frictionless data flows – Determining ownership, providing adequate protection, and fostering community trust are key to unlocking the economic potential of data. While data ownership is governed by the Copyright Act, data protection is the subject of the yet unenacted Personal Data Protection Bill. Provisions intended to foster trust are however absent from these. The IT Act can fill this gap by creating a framework to ensure data integrity and facilitate frictionless flows of data. This may be achieved by making statutory provisions for technical interoperability, data portability, data provenance, and alternative data sharing models like federated learning and data trusts.

Consider creating a data ethics framework – Fostering community trust goes beyond statutory safeguards. The ever expanding uses of data raise moral and ethical questions that may not be addressable through laws. An emerging method used to safeguard trust without burdening businesses or stifling innovation through over-regulation is to create a data ethics framework: a set of principles that guide the appropriate and responsible use of data. Key elements of such a framework may include: maintaining transparency in the use of data, mandating businesses to formulate a data ethics policy, and incentivising data ethical business models and data sharing practices.

Chapter IV – Encryption and Law Enforcement Access

Encryption regulation should strike a balance between privacy and law enforcement – Encryption is an important tool for ensuring individual privacy and securing sensitive business information. Yet it makes it difficult for law enforcement agencies to intercept communication for lawful reasons like controlling the spread of misinformation, checking online piracy, and apprehending criminal activity. It is important to strike a balance between individual privacy and the state's duty to maintain law and order. This can be ensured through procedural checks and balances aimed at curbing the misuse of surveillance powers.

Lawful interception without compromising encryption standards is desirable – Two broad approaches are seen internationally in encryption regulation. Countries like Australia prefer the 'backdoor' approach, which relies on weakening encryption standards by introducing system vulnerabilities that allow ready access when needed. Countries like Germany prefer to build state capacity to hack devices, with a legal framework tailored to support such operations. The encryption framework in the IT Act would better emulate the latter model.

Chapter V – Access and Blocking

Hardwire checks and balances into the statute to prevent misuse – Section 69A of the IT Act and the rules framed under it are overbroad and vulnerable to overuse or misuse. To prevent abuse, the statutory provisions must be ring-fenced by procedural safeguards. Primarily, blocking orders must be used as the last resort. Such actions should also be proportional, temporary, transparent and must pass the muster of due process. Global best practices codified in judicial pronouncements and international law can be used to create a holistic framework for India

Chapter VI – Cybersecurity

Expand the definition of cybersecurity – The definition of cybersecurity merits a reconsideration to expand its scope. It is non-compliant with the Confidentiality Integrity Availability or CIA triad, the gold standard of information security. It is also limited in scope and may not cover the ever expanding ecosystem of the Internet of Things, a prominent theatre in the emerging cyberthreat landscape.

Offences should be redefined to expand their scope and prescribe stricter sanctions – The existing approach to criminalising conduct that may jeopardise the security and integrity of cyberspace is limited in scope and lacks deterrent power. Section 43, which punishes the offence of unauthorised access, does not criminalise acts emanating from the unlawful use of authorised access. Sanctions under the provision are limited moreover to compensatory penalties. This is less stringent than in other jurisdictions and also leaves scope for judicial discretion. Similarly, while Section 66 of the Act provides for aggravated forms of the offences defined in Section 43, it is premised on the threshold of dishonest and fraudulent intent borrowed from Indian Penal Code. These conceptions are more than a century old and are not fit for application in cyberspace.

Consider a centralised, multi-stakeholder organisational framework – The IT Act created two separate cybersecurity agencies: the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In). While the NCIIPC is tasked with protecting India's critical infrastructure CERT-In deals with non-critical sectors. Jurisdictions like the UK, the US and Singapore on the other hand rely on a central agency to govern all aspects of cybersecurity. Responding to cyberattacks is a time-sensitive exercise and the existence of multiple agencies may reduce response time. Further, cybersecurity is a joint imperative, served best by a multi-stakeholder approach. A future framework must facilitate closer cooperation with non-government stakeholders including industry and academia.

Notes

1 Sections 65–71, Information Technology Act 2000

2 Fifteenth Report, Standing Committee on Information Technology (2007-2008), Fourteenth Lok Sabha, Ministry of Communications and Information Technology

3 Section 69, Information Technology Act 2000

4 Steve Jones, Why 'Big Data' is the fourth factor of production. Financial Times, December 27, 2012. https://www.ft.com/content/5086d700-504a-11e2-9b66-00144feab49a

5 Government plans new IT Act to factor in crime, data privacy, new tech. https://www.livemint.com/industry/infotech/plan-to-revamp-it-act-ravi-shankar-prasad-11582716511721.html

6 Reserve Bank of India, Survey on Computer Software and Information Technology-Enabled Services Exports: 2018-19, 18 November 2019, https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR12100F173C491E344D91A3E10081354E0613.PDF

7 NASSCOM, Indian Tech Startup Ecosystem, https://www.nasscom.in/system/files/secure-pdf/NASSCOM_Startup_Report_2019_05112019.pdf

8 LiveMint, Indian IT Industry set to invest big in automation, AI in 2019, https://www.livemint.com/Companies/7SCOBS4thwVTTVs18quUlL/Indian-IT-industry-set-to-invest-big-in-automation-AI-in-20.html

9 India Today, https://www.indiatoday.in/magazine/business/india/story/20130325-bpo-industry-call-centre-culture-dying-in-india-762765-1999-11-30; Quartz India, https://qz.com/india/1152683/indian-it-layoffs-in-2017-top-56000-led-by-tcs-infosys-cognizant/

10 CISCO Annual Internet Report 2018-2023, https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/air-highlights.html

11 NITI Aayog, AIRAWAT: AI Specific Cloud Computing Infrastructure, January 2020 https://niti.gov.in/sites/default/files/2020-01/AIRAWAT_Approach_Paper.pdf

12 Census of India 2011

13 Dr Christopher Decker, Goals-Based and Rules-based Approaches to Regulation, BEIS Research Paper Number 8, May 2018. Department for Business, Energy and Industrial Strategy, Government of UK. https://www.econstor.eu/bitstream/10419/196215/1/2018-08-regulation-goals-rules-based-approaches.pdf

14 The CPTPP is a free-trade agreement between Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore and Vietnam. Text available at https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/

15 US–Japan Digital Trade Agreement, available at https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf

16 Japan–Mongolia Free Trade Agreement, available at https://www.mofa.go.jp/files/000067716.pdf

17 The Consumer Protection Act, 2019, available at http://egazette.nic.in/WriteReadData/2019/210422.pdf

18 The Draft National E-Commerce Policy, available at https://dipp.gov.in/sites/default/files/DraftNational_e-Commerce_Policy_23February2019.pdf

19 WTO, Work Programme on electronic commerce, available at https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm

20 Chapter 10 of the India–Singapore Comprehensive Economic Cooperation Agreement, available at http://commerce.gov.in/writereaddata/trade/ceca/ch10.pdf

21 Article 14.1 of the Comprehensive and Progressive Agreement for Trans Pacific Partnership, available at https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf

22 Article 15.9 of the Korea–US FTA, available at https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf

23 Chapter 14, Article 1 of the Singapore–Australia FTA, available at https://dfat.gov.au/trade/agreements/in-force/safta/official-documents/Documents/safta-chapter-14-171201.pdf

24 As pointed out by multiple stakeholders in their response to the public consultation, see https://meity.gov.in/comments-invited-draft-intermediary-rules

25 Section 2(1)(w) of the IT Act defines an intermediary to mean 'any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes.'

26 Karishma Mehrotra, IT rules to separate social media firms, other online platforms, Indian Express, January 16, 2020, https://indianexpress.com/article/technology/social/it-rules-to-separate-social-media-firms-other-online-platforms-6218697/

27 Government of India (Allocation of Business) Rules, 1961, available at https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_2229.pdf

28 Notification 3787, Cabinet Secretariat, September 24, 2018, https://cabsec.gov.in/writereaddata/allocationbusinessrule/amendment/english/1_Upload_1508.pdf

29 I.d 74

30 Economic Times, 'MeitY Miffed at Ministries' sectoral data policies ahead of privacy law', available at https://tech.economictimes.indiatimes.com/news/internet/meity-miffed-at-ministries-sectoral-data-policies-ahead-of-privacy-law/68663254

31 Economic TImes, 'Efforts on to line up e-Commerce and data laws', available at https://economictimes.indiatimes.com/news/economy/policy/efforts-on-to-line-up-e-Commerce-data-laws/articleshow/74922822.cms

32 Committee of Experts on Data Governance, available at https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf

33 Report by the Committee of Experts on Non-Personal Data Governance Framework, available at https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

34 Model Framework for Guidelines on e-Commerce, available at https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Guidelines%20on%20e-Commerce.pdf

35 TRAI, Consultation Paper on Regulatory Framework for OTT Services, available at https://trai.gov.in/sites/default/files/OTT-CP-27032015.pdf

36 Responses to TRAI Consultation on Regulatory FrameworK for OTT Services; available at https://trai.gov.in/consultation-paper-regulatory-framework-over-top-ott-services

37 TRAI, Recommendations on Regulatory Framework for OTT Services, available at https://www.trai.gov.in/sites/default/files/Recommendation_14092020_0.pdf

38 Hagemann, Ryan and Huddleston, Jennifer and Thierer, Adam D., 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (February 5, 2018). Colorado Technology Law Journal. Available at https://ssrn.com/abstract=3118539

39 The International Telecommunication Union, 'Regulatory Approaches and Challenges in the New ICT Ecosystem', available at https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT03-2018-PDF-E.pdf

40 See Draft Central Consumer Protection Authority (Prevention of Misleading Advertisements and Necessary Due Diligence for Endorsement of Advertisements) Guidelines, 2020, available at https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20guidelines%20for%20stakeholders%20consultation.pdf

41 Ibid.

42 Business Standard, 'New Standing Committee of Secretaries on e-Commerce starts deliberations', available at https://www.business-standard.com/article/economy-policy/new-standing-committee-of-secretaries-on-e-Commerce-starts-deliberations-118091400027_1.html

43 Draft Drugs and Cosmetics Amendment Rules, 2018, Ministry of Health and Family Welfare, August 28, 2018, https://cdsco.gov.in/opencms/opencms/system/modules/CDSCO.WEB/elements/download_file_division.jsp?num_id=MTkzOQ==

44 The Drugs and Cosmetics Rules, 1945, http://vbch.dnh.nic.in/pdf/Rules%20and%20regulations%20of%20Drug%20and%20Cosmetics%20act.pdf

45 Garima Bora, Unclear regulations on e-pharmacies may hinder investments: 1mg's Prashant Tandon, The Economic Times, January 27, 2020, https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/unclear-regulations-on-e-pharmacies-may-hinder-investments-1mgs-prashant-tandon/articleshow/73652797.cms?from=mdr

46 Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

47 Uncovering The Child Porn Distribution Epidemic On WhatsApp, Fight the New Drug, October 14, 2019. https://fightthenewdrug.org/uncovering-the-child-porn-distribution-epidemic-on-whatsapp/

48 Robert Graham, How Terrorists Use Encryption, CTC Sentinel, June 2016, Volume 9, Issue 6. https://www.ctc.usma.edu/how-terrorists-use-encryption/

49 Online Platforms' Moderation of Illegal content Online, Law, Practice and Options for Reform, European Parliament, June 2020

50 OECD report on 'Alternatives to Traditional Regulation', available at https://www.oecd.org/gov/regulatory-policy/42245468.pdf

51 Stop Enabling Sex Traffickers Act and Allow States and Victims to Fight Online Sex Trafficking Act

52 Eliminating Abusive and Rampant Neglect of Interactive Technologies Bill

53 EARN It Act is ostensibly a bill to prevent sexual exploitation of children online, but critics say it could end internet privacy and encryption features. GovTrack, April 9, 2020. https://govtrackinsider.com/earn-it-act-is-ostensibly-a-bill-to-prevent-sexual-exploitation-of-children-online-but-critics-c01ed5b06ead

54 Executive Order on Preventing Online Censorship, Issued on May 28, 2020 https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/

55 John Koetsier, Trump's Executive Order Is 'Illegal,' Section 230 Author Says. Forbes, May 28, 2020. https://www.forbes.com/sites/johnkoetsier/2020/05/28/trumps-executive-order-is-illegal-section-230-author-says/#6401b4c36703

56 US Department of Justice, Section 230 - Nurturing Innovation or Fostering Accountability?, Key Takeaways and Recommendations, June 2020, available at https://www.justice.gov/file/1286331/download

57 Vinay Kesari, Intermediaries in India may be on the cusp of a brave new world. Factor Daily, September 17, 2018. https://factordaily.com/intermediary-liability-in-india-brave-new-world/

58 Indian govt asks WhatsApp to trace messages with fingerprints, Entrackr, June 18, 2019. https://entrackr.com/2019/06/india-asks-whatsapp-to-finger-print-messages/

59 K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

60 The definition of an intermediary, in Indian law, includes any person who receives, stores, transmits or provides any service with respect to a particular electronic record, on behalf of another person.

61 Section 1(1) of Telemediengesetz.

62 The Telecommunications Act 1997 separately defines carriage service providers and content service providers.

63 McCann FitzGerald, Proposed New EU Regulation for Intermediary Service Providers - The Digital Services Act, Lexology. https://www.lexology.com/library/detail.aspx?g=40cda5fb-8801-4255-acff-3f703ef619ec

64 Billy Perrigo, How the E.U's Sweeping New Regulations Against Big Tech Could Have an Impact Beyond Europe. Time Magazine, December 15, 2020. https://time.com/5921760/europe-digital-services-act-big-tech/

65 Network effect refers to the phenomenon that takes place when a platform links multiple sides of a market in ways that are increasingly valuable to those on one side as the number of participants on the other side increases. For instance, Facebook connects users to advertisers, and the greater number of users, the greater value for potential advertisers.

66 Janosch Delcker, Germany's balancing act: Fighting online hate while protecting free speech. Politico, October 1, 2020. https://www.politico.eu/article/germany-hate-speech-internet-netzdg-controversial-legislation/

67 In Shreya Singhal the Supreme Court struck down Section 66A of the IT Act. This provision made it an offence to send messages grossly offensive, known to be false, sent to cause annoyance, inconvenience, danger, insult, injury, hatred or ill will. The court held that terms such as annoyance and ill will are exceedingly broad in their scope and consequently the provision is vague and therefore in excess of reasonable restrictions on free speech.

68 Shreya Singhal v. Union of India, Global Freedom of Expression, Columbia University. https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/

69 Billy Perrigo, How the E.U's Sweeping New Regulations Against Big Tech Could Have an Impact Beyond Europe. Time Magazine, December 15, 2020. https://time.com/5921760/europe-digital-services-act-big-tech/

70 Tax and Digitalisation, OECD Policy Note, October 2018. https://www.oecd.org/tax/beps/tax-and-digitalisation-policy-note.pdf

71 Removals under the Network Enforcement Law, Google Transparency Report https://transparencyreport.google.com/netzdg/youtube?hl=en

72 Specific knowledge and actual knowledge are discussed in the following section.

73 Protection from Online Falsehoods and Manipulations Act, 2019

74 Revenge Porn Prevention Act, 2014

75 WCD proposes amendments to widen the scope of Indecent Representation of Women (Prohibition) Act (IRWA), 1986, Press Information Bureau, Press Release dated June 04, 2018. https://pib.gov.in/newsite/PrintRelease.aspx?relid=179754

76 Mary Hui, Singapore's fake news law is facing its first real challenge in court. Quartz, January 15, 2020. https://qz.com/1784632/singapore-faces-legal-challenge-over-fake-news-law/

77 Shreya Singhal v. Union of India (2013) 12 SCC 73

78 Myspace v. Super Cassettes 236 (2017) DLT 478

79 Kent RO Systems v. Amit Kotak & Ors. 240 (2017) DLT 3

80 Available at https://eur-lex.europa.eu/eli/dir/2019/790/oj

81 Heather Burns, The Digital Single Market and Brexit. After Brexit, June 24, 2020 https://afterbrexit.tech/digital-single-market/

82 Philipp Grüll, One year of EU copyright reform: Is the Internet still working?. Euractiv, April 20, 2020 https://www.euractiv.com/section/digital/news/one-year-of-eu-copyright-reform-is-the-internet-still-working/

83 Online Platforms' Moderation of Illegal Content Online, study requested by the IMCO Committee, European Parliament

84 Digital regulation: Designing a Supranational Legal Framework for the Platform Economy, Michele Fincl, LSE Law, Society and Economy Working Papers 15/2017, LSE Law Department

85 Intermediaries such as ISPs must pass on copyright infringement notices from rights holders to users to inform them that they are participating in copyright infringing activities such as illegally downloading films.

86 Intermediaries are required to forward any notice they receive of alleged illegality to the content provider, and wait for a predetermined period such as a week. If the content provider either consents or does not respond to the request, the material in question may be blocked or taken down. This gives the user providing the content the chance to respond.

87 The primary perpetrators of illegal content may be suspended from the intermediary's platform after having been given notice to prevent repeat offences in cases of hate speech.

88 Barton Swaim, 'The Twenty-Six Words That Created the Internet' Review: Protecting the Providers. The Wall Street Journal, August 19, 2019. https://www.wsj.com/articles/the-twenty-six-words-that-created-the-internet-review-protecting-the-providers-11566255518

89 Jeff Desjardins, How much data is generated each day? World Economic Forum. Available at - https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

90 Thomas C. Redman, Bad Data Costs the U.S. $3 Trillion Per Year. Harvard Business Review https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year

91 Annie Brown, Biased Algorithms Learn From Biased Data: 3 Kinds Biases Found In AI Datasets. Forbes. https://www.forbes.com/sites/cognitiveworld/2020/02/07/biased-algorithms/#159f693576fc

92 Insights Network Study Shows US Consumers Want Privacy and Protection of Personal Data https://martechseries.com/analytics/data-management-platforms/privacy-and-regulations/insights-network-study-shows-us-consumers-want-privacy-protection-personal-data/

93 S.806 - Own Your Own Data Act. https://www.congress.gov/bill/116th-congress/senate-bill/806

94 Cameron F. Kerry and John B. Morris, Jr. Why data ownership is the wrong approach to protecting privacy. Brookings Institution https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/

95 Report by the Committee of Experts on Non-Personal Data Governance Framework. Ministry of Electronics and Information Technology, Government of India.
https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

96 Teresa Scassa, Data Ownership. CIGI Papers No. 187 — September 2018. Centre for International Governance Innovation.
https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf

97 Hummel, P., Braun, M. & Dabrock, P. Own Data? Ethical Reflections on Data Ownership. Philos. Technol. (2020). https://doi.org/10.1007/s13347-020-00404-9

98 The Supreme Court of India in its judgement in Eastern Book Company & Ors. v. D.B. Modak & Anr. adopted the 'modicum of creativity' doctrine, propounded by the US Supreme Court in Feist Publications, Inc., v. Rural Telephone Service Co.

99 Justice K.S.Puttaswamy(Retd) vs Union Of India, Supreme Court of India, Writ Petition (Civil) No. 494 of 2012. https://indiankanoon.org/doc/127517806/

100 Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3

101 Exploring International Data Flow Governance Platform for Shaping the Future of Trade and Global Economic Interdependence. World Economic Forum White Paper, December 2019. http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf

102 Casalini F. and Lopez Gonzalez J. (2019), Trade and Cross-Border Data Flows, OECD Trade Policy Papers, No. 220, OECD Publishing, Paris: p. 15.

103 Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Chapter 14. https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf

104 A Roadmap for CrossBorder Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy. White Paper, World Economic Forum and Bahrain Economic Development Board, June 2020. http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

105 Guidance on Data Ethics Framework, Government of the United Kingdom https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework

106 Data for the Benefit of the People: Recommendations from the Danish Expert Group on Data Ethics. November 2018 https://eng.em.dk/media/12209/dataethics-v2.pdf

107 Kevin Granville, Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. The New York Times, March 19, 2018. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

108 Carole Cadwalladr and Emma Graham-Harrison, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

109 Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, Machine Bias. ProPublica, May 23, 2016 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

110 Collaborative machine learning without centralising training data, available at https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

111 Robert Graham, How Terrorists Use Encryption, CTC Sentinel, June 2016, Volume 9, Issue 6 https://www.ctc.usma.edu/how-terrorists-use-encryption/

112 What Is a VPN? - Virtual Private Network, CISCO https://www.cisco.com/c/en_in/products/security/vpn-endpoint-security-clients/what-is-vpn.html

113 Jason Hiner, Understanding Snowden's impact on IT... in 2 minutes. TechRepublic, November 26, 2013. https://www.techrepublic.com/blog/tech-sanity-check/video-understanding-snowdens-impact-on-it-in-2-minutes/#.

114 Sekwon Choi, How Netflix brings safer and faster streaming experiences to the living room on crowded networks using TLS 1.3. Netflix Technology Blog. https://netflixtechblog.com/how-netflix-brings-safer-and-faster-streaming-experience-to-the-living-room-on-crowded-networks-78b8de7f758c

115 Other laws such as the Indian Telegraph Act, 1885 and sector specific requirements that also regulate encryption are not within the purview of this chapter.

116 Section 69, Information Technology Act 2000

117 The Road Ahead for Encryption in India, NASSCOM–DSCI

118 Ivan Mehta, Report: India will force WhatsApp, Telegram to trace sensitive messages back to their originators. The Next Web, January 22, 2020. https://thenextweb.com/in/2020/01/22/report-india-will-force-whatsapp-telegram-to-trace-sensitive-messages-back-to-their-originators/

119 Bob Cromwell, Government-imposed backdoors make security much worse, not better. https://cromwell-intl.com/cybersecurity/backdoors.html

120 James Bamford, A Death in Athens: Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee. The Intercept, September 29, 2015. https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/

121 Ben Thompson, UAE Blackberry update was spyware. BBC, July 21, 2009 http://news.bbc.co.uk/2/hi/8161190.stm

122 Official Announcement about the Central Authority for Information Technology in the Security Domain, Transatlantic Cyber Forum, Policy Debates, January 31, 2017. https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DJanuar%E2%80%9D

123 German foreign spying law tested at top court, DW, January 14, 2020. https://www.dw.com/en/german-foreign-spying-law-tested-at-top-court/a-51997082

124 In their current form, the Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law, Press Release No. 37/2020 of 19 May 2020, Bundesverfassungsgericht. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html

125 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

126 Section 10, G-10

127 Ibid. Section 15

128 Ibid. Section 12

129 Ibid. Section 14

130 Issued under Schedule 7 of the Investigatory Powers Act, 2016

131 Interception of Communications: Code of Practice, March 2018. Home Office, Government of UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

132 Section 317ZG(1)

133 Assistance and Access: Common myths and misconceptions, Department of Home Affairs, Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act

134 Writ Petition (Civil) No. 494 of 2012

135 India's Surveillance State: Procedural Legal Framework, SFLC. https://sflc.in/indias-surveillance-state-procedural-legal-framework

136 Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, PRS Legislative Research. https://www.prsindia.org/billtrack/draft-information-technology-intermediaries-guidelines-amendment-rules-2018

137 Draft Encryption Policy https://www.huffingtonpost.in/2015/09/22/draft-encryption-policy_n_8174870.html

138 Unstarred Question No.2843, Lok Sabha, March 11, 2020.
http://164.100.24.220/loksabhaquestions/annex/173/AU2843.pdf

139 The Internet in China. Information Office of the State Council of the People's Republic of China June 8,2010. http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207983.htm

140 Over 14000 websites blocked by MEITY. Software Freedom Law Center, July 01, 2019. https://sflc.in/over-14000-websites-blocked-meity

141 Unstarred Question No. 1640, Rajya Sabha, available at https://pqars.nic.in/annex/251/Au1640.pdf

142 Pornhub Records 95 Percent Increase in Traffic from India amid 21-Day Lockdown. News18, April 06, 2020. https://www.news18.com/news/buzz/pornhub-records-95-percent-increase-in-traffic-from-india-amid-21-day-lockdown-2566267.html

143 Juraci Paixao Kroehling, Why IP-Based Rules Are Bad, but We Still Use Them. DZone, February 01, 2018. https://dzone.com/articles/why-ip-based-rules-are-bad-but-we-still-use-it

144 Danaher, Brett and Smith, Michael D. and Telang, Rahul, 'Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior' (April 18, 2016). Available at https://ssrn.com/abstract=2766795 or http://dx.doi.org/10.2139/ssrn.2766795

145 It is important to point out that Section 75 of the IT Act has extraterritorial application. Offences or contraventions committed outside India can be prosecuted under the Act if it involves a computer located in India. Rule 8(3) of the IT Rules 2009 provides for mechanisms through which notice may be served on foreign entities before an action under Section 69A is initiated against them.

146 Rules 7 and 8, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

147 Ibid. Rule 9

148 Ibid. Rule 16

149 International Covenant on Civil and Political Rights, United Nations Human Rights Committee, 102nd Session Geneva, 11-29 July 2011. General comment No. 34.
https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

150 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations General Assembly, May 16, 2011.
https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

151 International Covenant on Civil and Political Rights https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

152 Under Article 19(3) these are (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals.

153 Russia—Measures Concerning Traffic in Transit, DS512, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm

154 Press Information Bureau, Press Releases dated June 29, September 02, and November 24, 2020. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206; https://pib.gov.in/PressReleasePage.aspx?PRID=1650669; https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335

155 Saudi Arabia—Measures concerning the Protection of Intellectual Property Rights, DS567; https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds567_e.htm

156 Freedom House, Freedom on the Net 2020: The Pandemic's Digital Shadow.
https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf

157 Javier Pallero and Deji Olukotun, Access Now condemns blocking of WhatsApp in Brazil. Access Now, December 17, 2015.
https://www.accessnow.org/access-now-condemns-blocking-whatsapp-brazil/

158 [2016] EWCA Civ 658

159 2019 FC 1432 (CanLII)

160 Internet Society Perspectives on Internet Content Blocking: An Overview. March 2017. https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/#_ftn9

161 Policy Recommendations: Internet Freedom. Freedom House. https://freedomhouse.org/policy-recommendations-internet-freedom

162 Response to Unstarred Question No. 2895, Lok Sabha, answered on March 11, 2020. Available at http://164.100.24.220/loksabhaquestions/annex/173/AU2895.pdf

163 The Global Threat Landscape Report, 2019, Subex. Available at https://www.subexsecure.com/pdf/reports/Threat-Landscape-Report-2019.pdf

164 The Global Risks Report, 2020, 15th Edition, World Economic Forum. Available at http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

165 Cyber Smart: Enabling APAC Businesses, 2019, VMWare and Deloitte Access Economics. Available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/company/vmw-cyber-smart-enabling-apac-businesses.pdf

166 The International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2018. Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

167 Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Department of Banking Supervision, Reserve Bank of India.
https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf

168 Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

169 The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025. International Data Corporation, June 18, 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45213219

170 Leading the IoT: Gartner Insights on How to Lead in a Connected World. Gartner Research, 2017. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

171 Karen Lewis, IoT Security vs. IT Security: What's the difference?. IBM Blogs, November 18, 2016. https://www.ibm.com/blogs/internet-of-things/security-iot/

172 Conventional IT devices such as smartphones or computers are meant for personal use. They are either in a single user's possession or remain in the confines of secured spaces like users' homes or offices. IoT devices on the other hand may be placed in unsecured locations and in full public view. IoT enabled smart trolleys used at airports are a prime example.

173 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. National Institute of Standards and Technology, US Department of Commerce. Available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

174 Foundational Cybersecurity Activities for IoT Device Manufacturers, National Institute of Standards and Technology Interagency or Internal Report 8259, May 2020. Available at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

175 1.81.26. Security of Connected Devices, Senate Bill No. 327 Chapter 886. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

176 Code of Practice for Consumer IoT Security, Department for Digital, Media, Culture and Sports, Government of the United Kingdom. October 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

177 Code of Practice: Securing the Internet of Things for Consumers. Commonwealth of Australia 2020. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

178 Internet of Things (IoT) Cyber Security Guide (Version 1.0, March 2020), Infocomm Media Development Authority (IMDA). https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf?la=en

179 Press Information Bureau, Press Release dated August 29, 2005. https://www.prsindia.org/uploads/media/Information%20Technology%20/bill93_2008122693_Press_Release_for_IT_Act_Amendment.pdf

180 Regina v. Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America (on Appeal from a Divisional Court of the Queens Bench Division). [2002] 2 AC 216 https://publications.parliament.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm

181 'Insider unauthorised use of authorised access: What are the alternatives to the Computer Misuse Act 1990?' International Journal of Law, Crime and Justice, March 2016. DOI: 10.1016/j.ijlcj.2016.08.003

182 Reforming the Computer Misuse Act 1990: Criminal Law Reform Now Network Report, March 2020. http://www.clrnn.co.uk/publications-reports

183 Press Information Bureau, Press Release dated August 29, 2005 https://pib.gov.in/newsite/erelcontent.aspx?relid=11670

184 Global Cybersecurity Index, International Telecommunication Union. Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

185 Industry 100, National Cyber Security Centre. December 21, 2016 https://www.ncsc.gov.uk/information/industry-100

186 Saikat Datta, Defending India's Critical Information Infrastructure: The Development and Role of the National Critical Information Infrastructure Protection Centre (NCIIPC). Internet Democracy Project, March 2016. https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf