Data Governance Network

March 2020

Working Paper 06

Internet intermediaries and online harms: *Regulatory Responses in India*

Varun Sen Bahl, Faiza Rahman and Rishab Bailey

National Institute of Public Finance and Policy

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The National Institute of Public Finance and Policy (NIPFP) is a centre for research in public economics and policies. Founded in 1976, the institute undertakes research, policy advocacy and capacity building in a number of areas, including technology policy. Our work in this space has involved providing research and policy support to government agencies and contributing to the creation and dissemination of public knowledge in this field. Our current topics of interest include privacy and surveillance reform; digital identity; Internet governance and rights, and regulation of emerging technologies. We also focus on research that lies at the intersection of technology policy, regulatory governance and competition policy.

Terms of Use

Cover page credit: Cactus Communications

Paper design: Cactus Communications

Disclaimer

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organization.

Suggested Citation

Bahl, V. S., Rahman, F., & Bailey, R. (2020). *Internet Intermediaries and Online Harms: Regulatory Responses in India.* Data Governance Network Working Paper 06.

Supported by a grant from Omidyar Network

Abstract

The role played by Internet intermediaries in enabling or mitigating harmful conduct in the online ecosystem has garnered significant attention in recent policy debates, both globally and in India. In India, proposals to reformulate existing law and policy around this issue have been disaggregated. This paper attempts to examine recent attempts at regulating Internet intermediaries in India, with a view to answer three questions: first, what entities are being sought to be regulated, second, what are the harms that are driving calls for regulation, and third, what obligations are being imposed on Internet intermediaries to mitigate the said harms. We find that regulatory attempts have largely focused on a certain class of platforms in the content layer of the Internet, that are seen as posing significant risks to user safety. There appears to be a gradual move towards imposing greater obligations on certain types of intermediaries - though often the means and methods to do so is questionable. We therefore argue for a re-examination of the statutory framework pertaining to intermediary liability, to enable adoption of a differentiated/calibrated approach to regulating the online ecosystem, and to clarify the roles and responsibilities of different types of intermediaries therein.

Table of Contents

1. Introduction

The use of the Internet in India has increased dramatically in the past decade.[1] India is also one of the largest markets for many global technology companies in terms of user base.[2] While the increased use of the Internet has propelled the growth of the digital economy, and democratised access to information, it has also given rise to complex policy challenges surrounding the need to address harmful online content and conduct. At the heart of this challenge lies the issue of 'intermediary liability'. Should entities that transmit/carry/distribute third party (user) content, and enable online interactivity be held responsible for harmful acts that may be carried out on or using their services? The problem is one of balance: how to protect the fundamental rights of speech and expression of Internet users, the rights of intermediaries to carry on trade or business, whilst also ensuring the digital ecosystem is made safer for all users, and that harmful acts can be punished?

Against this background, this paper seeks to analyse the evolving regulatory approaches to addressing online harms in India, which to a large extent are disaggregated. To this end, we focus on the key drivers of regulation of the online ecosystem, and the measures adopted by regulators and the judiciary to address various online harms. We then try and identify and analyse trends that can inform future attempts at regulating intermediaries.

The paper is structured as follows: In the next section, we provide context to the debate around casting increased obligations on intermediaries, and outline the approach and limitations of this paper. The third section seeks to understand how existing law classifies different types of intermediaries, and if and how courts and regulators have attempted to either categorise intermediaries or cast specific obligations on different types of intermediaries. In the fourth section, we evaluate the evolving approaches to addressing seven categories of harmful online content/conduct. In particular, we focus

1 As of August 2019, India has 615.43 million broadband subscribers with 597.11 of them having wireless Internet access(Telecom Regulatory Authority of India, 2019). Approximately 12 percent of global internet users are from India, behind China's 21 percent (Grover, 2019).

2 For instance, India hosts the largest user base for WhatsApp and Facebook (Manish Singh, 2019) and (Statista, 2020).

on identifying various 'new' obligations imposed on intermediaries and the reasons for the same. In the final section of the paper, we analyse the trends highlighted in the previous section, with a view to understand and make recommendations regarding the future of intermediary regulation in India.[3]

2. Setting the scene: aim, approach and scope

In this section we provide context for the study conducted in this paper, and detail the approach and scope thereof.

2.1. Background

In India, the law pertaining to intermediaries is contained in Section 79 of the Information Technology Act, 2000 (IT Act), which provides all "intermediaries" with immunity from prosecution for carrying or transmitting user generated content, subject to the fulfillment of certain conditions. In order to avail this immunity, the intermediary should not have actively participated in the commission of the offence and should take remedial action upon gaining "actual knowledge" of the commission of the offence.[4]

Over the last decade, there has been increasing public debate over the need to continue providing such "safe harbour" to intermediaries, not least in view of the perception that multinational technology platforms are often slow to respond to issues of public safety, particularly in the developing world (Frosio, 2016), (Li, 2018). The push towards greater regulation, appears to derive primarily from two fault lines. First, the concern

3 The annexure to the paper discusses the key regulations that govern the operations of online intermediaries in India at present.

4 The purpose of this provision appears to be to extend the common law principle of distributors liability to the Internet. Generally, a distributor of illegal content in the physical world is not liable for the content, if she had no knowledge of it. On the other hand, a publisher, having knowledge and control of the illegal content, would be liable. In examining the rationale for introduction of the safe harbour provision, the Parliamentary Standing Committee examining the provision noted the representation of the Department of Information Technology, Government of India, which stated that the provision had been introduced as "...any of the service providers may not be knowing exactly what their subscribers are doing. For what they are not knowing, they should not be penalised. This is the provision being followed worldwide" (Parliamentary Standing Committee, 2007).

that (despite being increasingly regulated), the characteristics of the Internet imply that it continues to function as a space that is not yet fully subject to the rule of law. This fear is driven by the apparent rise in incidents of cyber-crimes.[5] Further, the emergence and increased awareness of a variety of online harms has led to concerns regarding the effectiveness of traditional law enforcement methods vis-à-vis the rapid pace of change of the digital ecosystem.

A second concern relates to the changing nature and business models of Internet intermediaries. Often certain intermediaries may not be acting in a completely "neutral" or "passive" manner. There are apprehensions that, inadvertently or otherwise, intermediaries may facilitate or exacerbate the scale and impact of harmful online activities (Gillespie, 2018). This raises questions of the continued utility of providing safe harbour to certain types of intermediaries - are intermediaries abusing safe harbour to avoid responsibilities owed to their users for the risks they face? Should they be required to "do more"? If so, what should they be doing?

These conversations have triggered a global movement towards casting greater responsibility on Internet intermediaries to ensure safety of users in the digital ecosystem.[6] For instance:

- In Germany, the Network Enforcement law (NetzDG) requires social media platforms with more than 2 million registered users in Germany to put in place procedures to expeditiously remove different types of illegal content.[7]
- In Australia, the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, 2019, imposes obligations concerning the need for certain classes

5 Recent statistics released by the National Crime Records Bureau for 2017 notes a 77 percent increase in the incidence of cyber crimes over the previous year. A total of 21,796 instances of cyber crimes were recorded in 2017 over 12,317 in 2016 and 11,592 in 2015 (National Crime Records Bureau, 2017).

6 Interestingly, many of these attempts are 'vertical' in nature i.e. apply to a specific class of intermediaries (as opposed to horizontal, which would apply across the board). See (Frosio, 2016).

7 The law, excludes intermediaries offering journalistic or editorial content and those enabling individual communication from its scope.

of intermediaries[8] to (a) inform authorities of abhorrent violent material being circulated using their services, and (b) act to remove such content expeditiously.[9]

- In New Zealand, the Harmful Digital Communications Act, 2015 sets out a range of court orders that can be served to intermediaries on referral from an approved agency, that specifically aims to target digital communications that cause "serious emotional distress". It also establishes an expedited mechanism for content takedowns within 48 hours.

- Arguably, the most elaborate regulatory response has come from the United Kingdom. The white paper on "Online Harms in the United Kingdom", seeks to establish a regulatory framework for a broad swathe of online intermediaries, that would cast a proportionate "duty of care" on these entities. The report bases the need for such a framework on the increasing instances of various 'online harms'.

Though regulatory efforts in India have to a large extent been disaggregated, there is no doubt that as with global trends, India too is seeking to cast increased obligations on various types of intermediaries to ensure safety of users in the digital ecosystem. Most notably, the central government has released a set of draft rules in December 2018, that seek to *inter alia* require intermediaries to use automated tools for content moderation, and enable the tracking of user generated content on their platforms.[10] While a number of provisions under the draft rules have been criticised by civil society and industry, the government's proposal to re-evaluate the legal obligations placed on intermediaries follows a long line of evolving judicial and regulatory approaches to tackling online harms.

2.2. Approach of this paper

This paper seeks to examine the evolving regulatory and judicial approaches to addressing online harms in the Indian digital ecosystem. The aim is to map and analyse recent

8 The law applies to (i) internet service providers, (ii) content service providers, and (iii) hosting service providers.
9 Violent material is defined as video or audio content depicting terrorist acts, murders, attempted murders, torture, rape or kidnap.
10 See the draft Information Technology (Intermediary Guidelines) Rules, 2018.

trends that can inform the future of the country's online content moderation and intermediary liability frameworks. To this end, we seek to address the following questions:

1. **Which actors are the primary focus of regulatory attention?** The term "intermediary", being defined very broadly defined in the IT Act, includes a large number of diverse entities that comprise the Internet ecosystem. In Section 3 we map the specific types/classes of intermediaries that have been the focus of regulatory attention. We examine how courts and regulators have either attempted to (or have failed to adequately) differentiate between types of intermediaries.
2. **What online harms has the State sought to address and how?** Section 4 focuses on identifying how courts and regulators/the government have attempted to address a range of online harms, and the nature of obligations imposed on intermediaries in these contexts. We seek to identify the rationale for imposing various obligations on relevant intermediaries and the means and methods adopted to do so.

   That said, we exclude a range of harms from our analysis. These include:

   - Privacy and cyber security related harms: While privacy related harms are one of the biggest risks in the online environment, we exclude such harms from the scope of our study. India is currently in the process of establishing a regulatory framework to deal with data protection related issues. We also exclude harms caused due to breach of cyber security, hacking, spread of viruses and computer contaminants.
   - Financial and e-commerce related harms: We exclude e-commerce issues that relate to consumer protection, customs and excise, etc. As far as e-commerce platforms are concerned, the study focuses on intellectual property (IP) infringements and harms caused due to the listing or advertising of regulated/illegal goods and services by users. We also exclude, financial crimes and payment system related offences from the scope of our study.[11]

11 The study excludes certain harms that may involve intermediaries, but are typically not dealt with under the rubric

- Harms related to market structure: We focus on harms where intermediaries act as such, and not where they are directly involved in the commission of the offence or where their own actions as a company can lead to individual or social harm. We therefore exclude a range of harms such as those arising from competition issues in the digital ecosystem, taxation, foreign investment policy, etc.
- Harms experienced on the dark net: Our study focuses on the harms likely to be suffered by the general populace and on more commonly used platforms, as these are currently the focus of regulatory attention.
- Spam, network/traffic management, quality of service and other network level harms, which are typically dealt with under telecom sector specific regulation imposed by the Telecom Regulatory Authority of India.

3. **What new obligations are being imposed on intermediaries?** As highlighted in the Annexure, Indian law currently uses both the IT Act and certain sector-specific regulations to place a number of obligations on different types of intermediaries. Further, the Supreme Court in the landmark *Shreya Singhal v. Union of India case* (2016), held that in order to avail the immunity under Section 79 of IT Act, an intermediary is required to expeditiously remove or disable access to relevant content after either receiving a court order, or on receiving a lawful notification from the appropriate Government agency.
4. Therefore, finally in this paper, we analyse the 'new' obligations, being imposed on intermediaries, outside of the abovementioned framework, with a view to understand the emerging contours of intermediary regulation in India, and make suggestions as to its future development.[12]

of content moderation. This includes harms such as violent crimes committed in the context of ride sharing applications and delivery services, the adulteration of food by restaurants using digital delivery services, fraud committed by e-commerce platforms, etc.

12 Note that a brief overview of existing obligations cast on intermediaries is provided in the Annexure to this paper.

3. Who is being regulated?

In this section we examine how the current regulatory framework in India understands the role played by different intermediaries in the digital ecosystem.

3.1. Defining "intermediaries"

The general meaning of an "intermediary" is a person who acts as a mediator between two parties, a messenger, a go-between.[13] Section 2(w) of the IT Act, defines an 'intermediary' as *"any person who receives, stores or transmits an electronic record, or provides a service with respect of that record, on behalf of another person."*[14]

The definition is therefore extremely broad - any participants in the online ecosystem, across the layers of the Internet, who transmit/carry or in any way provide a medium of access to and distribution of third party content, are included within its ambit. This definition does not attempt to classify or segregate intermediaries in any way.

However, as recognised by the wide-ranging list of intermediaries in the definition, intermediaries can be of many different types, each providing a different functionality in the online environment. Many are not visible to the user (for instance root servers, internet exchange points, gateways, backhaul providers etc.). These intermediaries assist in the delivery of communications from one node to another but do not themselves directly interact with the content or even the user. On the other hand some intermediaries, such as cyber cafes and wi-fi hotspots, merely provide a location for accessing online services. Others such as internet service providers provide a range of services from transporting to routing data. These can be differentiated from those that actively host information or take the form of social media platforms or communication apps where users can interact (such as WhatsApp, Facebook, Instagram, cloud-based services, etc).

13 Perset (2010) defines the term as referring to actors who bring together or facilitate transactions between third parties on the Internet. This includes a broad array of service providers who act "on behalf of' others, whether to provide Internet access services, enable the storage of data or facilitate the exchange of user-generated content.

14 The provision includes an illustrative list of intermediaries – telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

3.2. Categorising intermediaries

Typically, intermediary regulation the world over imposes obligations based on the function performed by the service provider.[15] This may be either in terms of their specific technical role in the Internet ecosystem or based on the business-model of the particular entity.

To illustrate, one may consider the European Union's E-Commerce Directive, 2000, on which Section 79 of the IT Act is modeled ('Directive of the European Parliament and of the Council on electronic commerce', 2000). The Directive categorises intermediaries into three distinct categories: (i) intermediaries that act as mere conduits,[16] (ii) intermediaries that provide caching services,[17] and (iii) intermediaries that provide hosting services.[18] The directive goes on to set out a range of differentiated obligations for each category of intermediaries as a pre-condition to availing the safe harbour from liability for third party content.[19]

The IT Act borrows from the above and as detailed in the Annexure, exempts intermediaries (a) providing temporary storage or transmission functions, (b) those that do not initiate/select the receiver of the transmission or select or modify the information in the transmission, from liability for third party content.

15 The US is traditionally considered to be an outlier in this regard, as the Communications Decency Act of 1996 and the Digital Millennium Copyright Act of 1998 conferred safe harbours on all intermediaries irrespective of functionality. However, as discussed later in this section, subsequent legislations have focused on increasing targeted obligations on specific services, such as in the context of protecting children.

16 Services whose functions consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network (Article 12).

17 Services whose functions consists of transmission in a communication network of information provided by a recipient of the service (Article 13).

18 Services whose functions consists of the storage of information provided by a recipient of the service(Article 14).

19 In order to avail of the safe harbour mere conduit intermediaries must not initiate the transmission, select the receiver of the transmission and select or modify the information contained in the transmission. Cache providers must not modify the information, must comply with conditions on access to the information, must comply with rules regarding the updating of the information, must not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information, and they must act to expeditiously remove or to disable access to the information it has stored upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Finally, in order to claim safe harbour, hosts should not have actual knowledge of the illegal act and, as regards claims for damages, should not be aware of facts or circumstances from which the illegal activity or information is apparent; and upon obtaining such knowledge or awareness, must act expeditiously to remove or to disable access to the information.

The above classification is however fairly basic in nature. A more detailed form of function-based classification of intermediaries is provided by Perset (2010).[20] Table 1 draws from this classification to provide an outline of the Indian landscape of intermediaries.

More recently, various jurisdictions have attempted to place specific obligations on narrower classes of intermediaries. This is notable for instance in the context of Germany and its NetzDG law which applies to large social media companies. Similarly, the UK's Online Harms White Paper, applies to a class of intermediaries that enable the exchange of user generated content or online user interaction (while excluding services that merely provide communication facilities - such as messaging and similar services). This would include intermediaries such as social media platforms, hosting sites, public discussion forums, messaging services and search engines of all sizes. However, the report clarifies that a new regulator constituted for

Table 1 Categories of intermediaries

Access services – Telecom and Internet service providers	
Provide access to the Internet to users	*Reliance Jio, Vodafone Idea, Atria Convergence Technologies, Hathway Cable & Datacom*
Web-hosting, data processing and content delivery	
Transform data, prepare data for dissemination, or store data or content on the Internet for others	*GoDaddy, Amazon Web Services, Microsoft Azure, Akamai*
Other intermediaries	
Internet search engines - Aid in navigation on the Internet	*Google, Bing, Yahoo*
E-commerce platforms - Enable online buying or selling	*Amazon, Flipkart, Uber*
Payment systems - Process Internet payments	*Visa, Mastercard, Paytm, Billdesk*
Participative networked platforms - Aid in creating content and social networking	– Social networking – *Facebook, Twitter, Linkedin* – Instant messaging – *Whatsapp, Skype* – Video content or file sharing – *Youtube, Vimeo, DailyMotion*

20 Also refer to Centre for Democracy and Technology (2012) for another function based classification of the intermediary landscape.

this purpose shall apply a risk-based and proportionate approach while imposing obligations i.e *"companies that pose the biggest and clearest risk of harm, to users, either because of the scale of the platforms or because of known issues with serious harms"* (Secretary of State for Digital, Culture, Media and Sport & Secretary of State for the Home Department, 2019).

Even in the United States, where all intermediaries are assured safe harbour from prosecution irrespective of their role in the network, different obligations have been imposed on specific classes of intermediaries based on a perceived social need. For example, the Children's Online Privacy Protection Act, 1998, is applicable to online services targeted at children below 13 years, where such service providers are based in the United States.[21] Similarly, many states within the United States have implemented laws regarding publicly funded schools and public libraries that require the adoption of Internet use policies and filtering mechanisms to prevent minors from gaining access to sexually explicit, obscene, or harmful material (Greenberg, 2018).

Jurisdictions across the world are therefore exploring ways of imposing differential obligations on different elements of the digital ecosystem. Countries such as Germany and the United Kingdom have chosen to impose additional regulations on specific classes of intermediaries such as social media platforms and intermediaries hosting user-generated content (Secretary of State for Digital, Culture, Media and Sport & Secretary of State for the Home Department, 2019), and (Federal Government of Germany, 2017). On the other hand, Australia and United States have opted to impose more horizontal obligations based on the severity of certain harms such as child pornography, sex trafficking and abhorrent violent material (Government of Australia, 2019) and (Government of the United States of America, 1998).[22]

21 The law requires such online services to setup and maintain procedures to protect the confidentiality, security, and integrity of children's personal information and obtain parental consent before collecting personal information of a child or allowing them to access facilities offered by the online service ('Children's Online Privacy Protection Rule', 2013).

22 The United States has also imposed obligations on certain classes of intermediaries under laws such as (Government of the United States of America, 2018).

3.3. Judicial and regulatory developments in India

Indian regulators are yet to adopt any holistic policy framework about an appropriate approach towards the classification of intermediaries.[23] That said, much government attention over the last few years has focused on specific classes of intermediaries (that would generally classify as 'hosts' in the previously discussed regulatory frameworks) in view of the enhanced nature of risks that such platforms ostensibly contribute towards. These include:

- "Social media platforms", such as Facebook, Twitter, Youtube, Sharechat, and TikTok[24]
- E-commerce and classifieds portals (such as Amazon, Flipkart, Olx, etc.)
- Communication platforms (such as WhatsApp and Telegram)
- Platforms that aid in the distribution of pornography (as identified by Government notifications from time to time)

Courts on the other hand have tended to focus on the parties arrayed before them in any specific matter and accordingly have generally avoided any detailed discussion on the need to classify different types of intermediaries. Most cases arising before the Indian courts have scrutinised certain types of intermediaries based on their role in contributing towards or enabling a specific harm - so we have noted some instances of intermediaries being treated as a "class" for instance, in the context of obligations being imposed on search engines to restrict access to pre-natal sex determination related content, or in the context of social media and communication services being used to spread 'fake news'.[25] Table 2 below broadly sets out the type of intermediaries prosecuted before Indian courts and the corresponding harms that provide the basis of the litigation.

23 The government has notified guidelines under Section 79 that are applicable only to a specific class of intermediaries. The Information Technology (Cyber Cafes) Rules, 2011 lay down specific obligations applicable only to cyber cafes. As detailed in the Annexure, the government has also applied data retention norms specifically to digital locker intermediaries.

24 See for example, (Ministry of Electronics and IT, 2018).

25 However, even in such cases, it is unclear to what extent obligations have been applied across the board, including to smaller or marginal service providers.

As highlighted in Table 2, it appears that certain types of harms are specifically raised before courts, with petitions focusing on arguing for more obligations to be imposed on specific types of intermediaries and platforms. We have seen multiple cases against e-commerce platforms in the context of intellectual property related harms,[26] social media platforms in the context of hate speech, defamation, sedition and similar harms,[27] etc. This is also apparent from a number of cases that have carved out new obligations in the context of a narrow set of particularly egregious harms such as (i) advertisement of pre-natal sex determination kits/services on search engines (Sabu Mathew George v. Union of India, 2017), (ii) child pornography and rape related content on pornographic websites and social media platforms (In Re: Prajwala, 2015), and (iii) intellectual property infringements on e-commerce platforms ('Christian Louboutin SAS v. Nakul Bajaj', 2018).

Table 2 Who is being litigated against?

Sr no.	Harm	Intermediaries
1.	Hateful, offensive and dangerous content	Social media (Twitter, Facebook), Communication apps (Whatsapp)
2.	Obscene content	Social media platforms (Facebook, TikTok), Pornographic websites, Communication apps (Whatsapp, Sharechat)
3.	Defamatory content	Social media platforms (Facebook, Twitter), Blogging platforms (Google), Video hosting platforms (Youtube, Instagram)
4.	Seditious and terrorism related content	Social media (Facebook, Twitter) and communication apps (Telegram, Whatsapp)
5.	Content harming democratic institutions	Communication apps (Whatsapp), Social media (Twitter, Facebook)
6.	IP infringements	E-commerce platforms (Amazon, Darvey's, kaunsa.com), Classifieds (Olx, etc.)
7.	Sale/advertisement of regulated goods and services	Search engines (Google, Yahoo) and intermediaries aiding sale/advertising of regulated goods or services (Dunzo, etc.)

26 See 'Christian Louboutin SAS v. Nakul Bajaj' (2018) and 'Amway India Enterprises Pvt. Ltd. v. 1MG Technologies Pvt. Ltd.' (2019)

27 See for example, (S. Muthukumar v. The Telecom Regulatory Authority of India, 2019) and ('Swami Ramdev v. Facebook', 2019)

Notably, we have not sighted any instances of regulatory action (pertaining to content moderation) against network layer intermediaries, such as telecom service providers or content delivery networks. While telecom service providers (TSPs) are frequently required to block urls or even shut-down the Internet altogether, there does not appear to be any specific regulatory developments in this regard that speak to the issue of intermediary liability. Our research indicates that most cases focus on remedies qua user-facing, content layer platforms.

Form the above, we see that any system of classification - such as it exists under the current regulatory framework - has arisen as a natural consequence of certain harms that are seen as occurring on certain types of platforms being brought before courts and regulators. The issue of classification of intermediaries takes on importance, as an approach that apportions responsibility based on risk prima facie appear to be more proportionate than an approach that requires all intermediaries to adopt similar policies. Given that proportionality is a requirement for judging the constitutionality of a law that infringes on fundamental rights such as that of expression and privacy, putting in place appropriately granular regulation therefore becomes essential. As greater obligations are cast on intermediaries, it makes sense therefore to target these obligations only at the specific classes of intermediaries where such measures are strictly required. Implementing obligations on a horizontal basis i.e. to all intermediaries, could also lead to problems with implementation in that generic obligations may not be implementable by all intermediaries (due to differences in function, capacity and business model). This may therefore lead to either disproportionate effects on the digital ecosystem or the imposition of obligations that are impractical or impossible to adhere to.

Consequently, in light of the multiplicity of functions performed by intermediaries, the distinct approaches being adopted by other jurisdictions, and the key concerns that have animated the call for regulation of intermediaries in India, it appears that any legal framework to address online harms, ought to incorporate a calibrated approach to casting obligations on intermediaries. A necessary first

step in this direction would therefore would be to clearly identify the main harm or a set of harms that need to be prevented or punished, and the relevant business models that enable these harms. Thereafter, it is advisable to put in place different responsibilities on different categories of intermediaries based on the nature/function/role of the intermediary and its perceived 'contribution' or ability to address a specific harm.

4. What online harms are being regulated, and how?

Understanding what constitutes a "harm" is in itself a complex philosophical and jurisprudential exercise. Ultimately, the issue of what types of conduct/content are considered important enough to regulate, as well as the manner of regulation, is one of finding a balance between the various values that a society attempts to inculcate and propagate.

In the context of the Internet, finding such a balance can be challenging not least due to the unique nature of the medium that can both enable the expression of fundamental liberties, while also creating new opportunities for individuals to be exposed to harms. Koops (2010) identifies 12 risk factors that make the Internet a "*unique opportunity structure for crime*", which include: (i) the global reach of the Internet, (ii) the deterritorialisation of criminal activity, (iii) decentralised and flexible networks, (iv) anonymity, (v) enabling of distant interaction, (vi) manipulability of data, (vii) automation of criminal processes, (viii) ability to scale criminal acts, (ix) ability to aggregate small gains, (x) enablement of an information economy, (xi) structural limitations to capable guardianship, and (xii) rapid innovation cycles.

The Internet therefore can magnify the risks an individual or society is exposed to. Further, threats to the safety and security of users are just as diverse as the risks a person may face offline. Harms can range from the more benign forms of annoyance and inconvenience to the distribution of content that can threaten national security

and endanger the physical safety of individuals and communities. Harms caused in the online environment also evolve rapidly as new technologies and services are introduced that change how users interact with one another. This makes it difficult to exhaustively list all or even most of the possible online harms. We also found no comprehensive taxonomy or categorisation of online harms in the Indian context - though international literature does offer some starting points.

For instance, the United Kingdom's Office of Communications (OFCOM) identifies (1) illegal speech (such as hate speech, child exploitation or incitement to terrorism) (2) age-inappropriate content (such as porn or graphic content) (3) other potentially dangerous content posing a significant risk of personal harm (such as imagery promoting self-harm or violence) (4) misleading content (such as fake news or misleading political advertising) and (5) personal conduct that is illegal or harmful (such as bullying, grooming or harassment) (Ofcom, 2018).

Literature also identifies six grounds on which speech restrictions are usually imposed in India: defamation; sedition and the use of national symbols; contempt of court; hate speech; morality; obscenity and sexual expression; and intellectual property rights (Kovacs & Nayantara, 2017).

Using this framework, this study concentrates on analysing a sub-set of online harms that have been been the focus of or that have provided the impetus for regulatory action pertaining to intermediaries. We examine statute, recent and ongoing litigation, draft and current policy documents, news reports and research studies to identify 7 broad thematic categories of *illegal and harmful* online activity:

1. Hateful, offensive and dangerous content
2. Obscene and sexually explicit content
3. Defamatory content
4. Content promoting sedition and terrorism
5. Content that interferes with democratic processes and institutions

6. Content that infringes intellectual property rights
7. Sale and advertisement of regulated goods and services

These harms are generally legislated against through a range of generic laws - such as the Indian Penal Code of 1860 (IPC); medium or sector-specific laws - such as the IT Act; and harm-specific laws (such as the Copyright Act, 1957, the Protection of Children from Sexual Offences Act, 2012, the Pre-Conception and Pre-Natal Diagnostic Techniques Act, 1994, and the Prevention of Insults to National Honour Act, 1971, etc.[28]

We also examine a final category of *new and emerging* harms, that are not captured in some way within existing law.

4.1. Hateful, offensive and dangerous content

One of the primary risks individuals face in the online space is of being exposed to 'hateful', 'offensive' or 'dangerous' content. India has numerous laws that regulate both online and offline speech on grounds that this may either hurt individuals or impact social harmony. Such content may broadly be divided into three categories.

- **Hateful, offensive and intimidatory speech:** Hate speech offences are criminalised under various laws, including under the IPC and certain special laws.[29] As recognised in the 267th report of the Law Commission of India, the issue of online hate speech is significant not only due to the size of the audiences who may be exposed to such content, but due to the real-world consequences that such speech can have (Law Commission of India, 2017).

28 Most of these laws apply equally to the online space as they would offline, though this may not be the case if: (a) there is a specific offence created under a special statute that applies to the Internet - say for instance in the case of Indian Penal Code provisions concerning obscenity, which are "overridden" by the punitive provisions in the IT Act, in recognition of the unique nature of the Internet as compared to traditional media; (b) due to the specific wording of statutes that sees them applied only to traditional media - for instance, in the case of the Indecent Representation of Women (Prohibition) Act, 1986, which is currently applicable only to traditional media and is therefore likely to be amended (PRS Legislative Research, 2013),(Press Trust of India, 2018c) and (Press Trust of India, 2018d).

29 The IPC proscribes intimidatory and harassing behaviour under Sections 503 and 354D. Further, Sections 153A or 295A, prohibit speech that promotes enmity between different groups on grounds of religion, race, place of birth, residence, language, and speech that intends to outrage religious feelings of any class by insulting its religion or religious beliefs respectively. In the context of protected communities, other legislations, such as the Scheduled Castes & Scheduled Tribes (Prevention of Atrocities) Act, 1989 may also apply.

We have come across a large number of cases relating to individuals posting hateful content online. For instance, individuals have been arrested for publishing casteist slurs on social media platforms;[30] for criticising religion/gods in social media posts[31] and making derogratory remarks against women.[32]

- **Spreading rumours/fake news:** The spreading of rumours (to create fear and panic amongst the public) is criminalised under Section 505 of the IPC.[33] As per recent statistics released by the NCRB, a number of persons have been arrested under this provision for spreading "fake news" online (Shakil, 2019). An increasing concern for the State, has been a rise in incidents of mob violence and lynchings because of the spread of rumours on messaging apps such as WhatsApp.[34]

- **Encouragement or abetment of self harm and suicide:** A rising concern amongst the public is the spread of online content that encourage selfharm or even suicide.[35] The Internet provides a platform for bullying and trolling, which can lead to incidents of self-harm or suicides. There are also a number of reports that point to individuals comitting suicide on live streaming services, often while being watched by large numbers of other users.[36] Such instances can, in addition to being harmful in and of themselves, also lead to copycat attempts (O. Singh, 2019). Harm can also occur due to the easy access the Internet provides to suicide related information or by actively promoting self-harm.[37]

30 See (Gayatri v. State, 2017).

31 See Parmeshwar Bharati v. State of U.P. (2018), Bijumon v. The State of Kerala (2018) and Ashwath v. The State (2017).

32 See 'S.Ve. Shekher v. Inspector of Police - Cyber Cell' (2018) where the Madras High Court refused to grant anticipatory bail to a politician accused of posting derogatory remarks against women on social media.

33 While we specifically contend with the issue of hateful rumours spreading on messaging apps in this section, the broader issue of "fake news" is dealt with in a subsequent section of this paper under the category of 'emerging harms'.

34 Around 40 deaths in between 2017-2019 have been attributed, to some extent, to the spread of rumours using digital communication apps such as WhatsApp (S. C. Agarwal, 2018), (P. K. Dutta, 2018), (Fazili, 2018), (Sanghvi, 2018), (McLaughlin, 2018), and (Safi, 2018). The rumours have been of child abductions, organ harvesting, cattle-thefts, cow-killings and beef consumption, all of which have encouraged violence against victims by vigilante mobs.

35 See for example, (Press Trust of India, 2017), (IANS, 2016), and (IANS, 2018a).

36 See for example, (S. Kumar & India Today Web Desk, 2019), (Abraham, 2018), (Goel, 2018), (Staff Reporter, 2018), (Natrajkumar, 2019) and (Times News Network, 2018).

37 As in the case of the Blue Whale game, the "choking challenge" or the "ice and salt challenge" (Baruah, 2017), (Chan, 2018), (Manglik, 2017), and (Desk, 2019).

In cases where the originators of such types of dangerous content can be found, they are often booked under general provisions that criminalise abetment of suicide or provisions barring hateful or obscene speech.[38] While some have suggested using AI and other solutions to scrutinise online communications for content that suggests or encourages self-harm, others have called for more drastic solutions, including a complete ban on live-streaming services (IANS, 2019) and (O. Singh, 2019). However, given the complexity of factors that can go into a case of suicide, there is no consensus on how the issue should be dealt with - including within the medical or academic community (Bhargava, 2018) and (Khattar, Dabas, Gupta, Chopra & Kumaraguru, 2018).

Regulatory developments

The response of the state to the above categories of content has usually been to block access thereto. This may also be followed by efforts to trace the individuals involved in publishing such content. Blocking is used particularly in the context of content that could lead to any communal or mob violence. For example, in 2012, the government ordered the blocking of access to over 300 pieces of content (urls, twitter accounts, blog posts, etc.) (Prakash, 2012). However, such attempts have faced criticism with some pointing out that the relevant orders were replete with egregious mistakes.[39]

Attempts at legislative intervention have come in the form of a private member's bill introduced in 2018, which sought to create a regulatory authority to oversee a series of proposed obligations on intermediaries.[40]

38 The Indian Penal Code, 1860, recognises an attempt to commit suicide as a punishable offence under Section 309. However, the Mental Healthcare Act, 2017, provides that a person who attempts to commit suicide shall not be tried and punished under the provisions of the IPC. Attempt to suicide is therefore virtually de-criminalised in India. Sections 306 and 107 of the Indian Penal Code, 1860, criminalise the abetment of suicide. Abetment of suicide can occur if a person instigates another to commit suicide, is part of a conspiracy to make a person commit suicide, or intentionally assists a person commit suicide by an act of ommission of commission.

39 These include for example, the suspension of accounts of people who were engaged in debunking rumours, inclusion of HTML tags in the list of content to be blocked (as opposed to web addresses or urls), blocking of entire domains instead of specific pieces of content, etc.(Prakash, 2012).

40 See Social Media Accountability Bill of 2018 (Mehrotra, 2018). It proposes establishing a Network Enforcement Authority to ensure that intermediaries follow through on their obligations under the Bill, such as the need to appoint specific officers to deal with complaints.

While there have been no actual amendments to the statutory framework, various other regulatory and judicial developments with respect to online hate speech have indeed taken place. For instance, a report by the TK Viswanathan Committee in 2017, suggested amending the IPC to include new provisions to specifically address the issue of online hate speech (Chisti, 2018).[41]

Much regulatory and judicial attention has primarily focused on the harms arising in two specific contexts - (a) the rise of communal/mob violence and lynchings fuelled by the propagation of online rumours, and (b) increasing instances of self-harm fuelled by dangerous online content.

- **Lynchings, mob violence and cyber-bullying:** The Supreme Court has dealt with the issue of lynchings and mob violence in two cases - Tehseen S Poonawalla v. Union of India (2018) and Film Society v. Union of India (2018). In the former, the Court advocated the introduction of a law to specifically deal with lynchings, and issued a series of "remedial, preventive and punitive measures" as directions to various officials across all levels of Government, including requiring them to "prohibit the dissemination of offensive material through social media platforms or any other means". In the latter case, the Court directed government authorities to *inter alia,* impose reasonable restrictions on social media and messaging services to control rumours. Interestingly, the Court, while observing that the uploaders of content should face appropriate criminal action, has not sought to extend any specific measures to platforms/intermediaries. However, recent developments indicate that this may no longer be the case, with communication apps such as WhatsApp coming under pressure to provide greater assistance to law enforcement agencies in enabling the tracing of uploaders of illegal content.[42]

41 The draft of the provisions released by media reports suggest that the report proposes a new provision in the IPC - 153C - which would penalise the using of a means of communication to incite hatred or gravely threaten a person or group of persons on the grounds religion, race, caste or community, sex, gender identity, sexual orientation, place of birth, residence, language, disability or tribe. The Committee has also proposed introduceding a new section 505(A) which would enable prosecution of conduct that causes fear, alarm or provocation of violence on the aforementioned protected grounds (Sebastian, 2017).

42 In 'Antony Clement Rubin v. Union of India' (2019) and 'Janani Krishnamurthy v. Union of India' (2019), the petitioners sought the linking of government issued identity cards with email addresses and user accounts. Their concern was the absence of action from the police and intermediaries to incidents of cyber-bullying, cyber defamation and cyber-stalking, particularly *"rising instances of humiliation, disgrace and defamation caused"* affecting the

The government too has increasingly discussed the possibility of casting greater obligations on intermediaries to regulate speech that could lead to lynchings. For instance, in 2018, an Expert Committee of Secretaries recommended:

— Holding intermediaries liable for not expeditiously blocking offensive / malicious content, when brought to their notice (V. Singh, 2018).[43]

— Improving interaction between intermediaries and law enforcement agencies to ensure more prompt compliance with legal orders to block content, and to enable more proactive monitoring of social media content by the authorities (and the intermediaries themselves).

— Using non-governmental organisations and volunteers to surf the Internet looking for objectionable content, which can then be reported to the intermediaries (who will be required to disable access thereto) (Express News Service, 2018).

Some social media platforms and communication apps have also been served with two advisories in July 2018 wherein the government requested them to *inter alia* take steps to identify and stop spread of viral messages that could incite violence; ensure accountability of users on their platforms including through proper means of tracing originators of illicit content; and ensure that they had an office located in India and would provide speedy assistance to law enforcement agencies when required to do so (S. C. Agarwal, 2018), (Anonymous, 2018), (IANS, 2018b), (Aggarwal, 2018a) and (Das & Gupta, 20 1 8).[44] However, the government's efforts in this regard have not been universally welcomed. Some have pointed out that by focusing on the medium used to disseminate such content, the government has ignored the opportunity to deal with the real source of the problem (Arun, 2019).

general public online. The division bench of the Madras High Court has expanded the scope of the lis to include issues of curbing cyber-crime and intermediary liability. The ongoing hearings have involved detailed discussions on WhatsApp's end-to-end encryption, the possibility of traceability, and the need for social media companies to work with law enforcement agencies to address cybercrime. The matter is currently pending in the Supreme Court in view of a transfer petition filed by Facebook.

43 A failure to do so could involve criminal proceedings being initiated against the country-heads of the intermediary involved (for non-compliance with relevant orders) (Pradhan, 2018).

44 WhatsApp in particular has come under pressure to re-design its platform to include the ability to to trace messages and determine how many times a message has been read or forwarded. Notably, some senior officials have stated that "*we have reached the limit of anonymity on the Internet and that has to go*" (Mandavia, 2019).

Most of the concerned intermediaries have responded by implementing technical measures to limit the spread of misinformation.[45] The efficacy of these measures however has been questioned by senior government officials, with the Minister for Communications and Information Technology making it clear that social media companies would be held responsible for failing to check illegal activities on their platforms (Prasad, 2018) and (Aggarwal, 2018b).[46]

- **Encouragement of self-harm and suicide:** Indian courts have had occasion to deal with the issue of content that encourages suicidal behaviour in the case of the online game known as the "Blue Whale challenge".[47]

  Worried by reports of the number of children harming themselves because of the game, the Blue Whale issue was brought up in Parliament in 2017, following which the government directed intermediaries to block access to the game (Tech2 News Staff, 2017) and (Mausami Singh, 2017). Individuals propagating the game were to be reported to the relevant authorities, while police and other government authorities were instructed to conduct greater scrutiny of social media, carry out awareness drives and provide counseling and helpline services.[48]

  The Madras High Court took up the matter suo-moto in 2017 in The Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications (2017). Upon considering the steps taken by various authorities to block access to the game as well as the responses of intermediaries such as Google, the Court observed that intermediaries had a responsibility to the public to ensure that illegal

45 Notably, WhatsApp has limited the number of forwards a user can send, added a button to indicate if a message is a forward, begun to work with fact checking services, and put in place local content moderation and management teams (Prasad, 2018), (Press Trust of India, 2018e), (Thaker, 2019) and (Reuters, 2019). Services such as Facebook have also begun to mark-out material that has been fact-checked (by third parties) and found to be false.

46 This would entail implementing relevant technical measures to screen and filter inappropriate/illegal content, trace originators of content etc., while also ensuring that they submit to the authority of Indian courts and law enforcement agencies - including by establishing local offices and appropriate grievance redress mechanisms (Prasad, 2018).

47 This 'game', in which youth are encouraged to undertake a series of self-harm related challenges leading up to suicide, is initiated in closed groups on online services but then largely 'played' through direct messages. Individuals are asked to commit a series of escalating self-harm based challenges ultimately leading to suicide (Khattar et al., 2018) and (UNICEF, 2017). The game has apparently lead to the death of atleast 5-10 individuals over the last few years (Adeane, 2019) and (Pathare, 2017).

48 Refer (Ministry of Electronics and Information Technology, 2017), (S. Agarwal, 2017) and (The Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications, 2017).

or harmful content should not be made available on the Internet. Accordingly, a series of directions were issued requiring *inter alia*:

— The central government to take appropriate legislative measures to ensure all "over the top services" and foreign based intermediaries were brought under the ambit of Indian law (or else, were blocked). The government was to ensure that the relevant laws were updated to enable law enforcement agencies to secure the timely assistance of intermediaries;

— Intermediaries to undertake due diligence to remove all links and hashtags being circulated on the Internet, and provide information regarding downloading of the game and suspicious URLs;

— Relevant websites to be blocked upon orders of the government; and

— Awareness creating measures to be undertaken by the relevant authorities.

The Supreme Court took up the issue not long after in Sneha Kalita v. Union of India (2017). Noting that blocking instructions had been issued to various intermediaries and that relevant government authorities were investigating the matter, the court primarily focused on ensuring that government authorities take steps to spread awareness of the issue amongst the vulnerable sections of the population.

4.2. Obscene and sexually explicit content

The relative ease with which the Internet has enabled the publication and transmission of various types of sexually explicit content, captured either consensually or non-consensually, has been a consistent concern of authorities in India.[49]

49 While countries have disagreed on the extent to which adult pornography may be banned, there is broad consensus globally on the need to address child porn(Arun, 2014) and (World Congress Against Sexual Exploitation of Children and Adolescents, 2008).

Indian law criminalises adult consensual and non-consensual pornographic content,[50] revenge pornography,[51] child pornography [52] etc. In addition, there are also distinct harms criminalised in law that pertain to online *conduct* that is sexually abusive or explicit in nature. These are often directed at vulnerable groups such as women, children, and sexual minorities.[53]

Judicial developments and regulatory practice

The two most important cases that deal with the issue of intermediaries' responsibility regarding the distribution of sexual explicit or pornographic content are that of Kamlesh Vaswani v. The Union of India (2018), which deals with the issue of online pornography, and In Re: Prajwala (2015), which deals with the circulation of child porn and rape videos.

The directions issued in the Prajwala case[54] are particularly important. Here, the Supreme Court directed intermediaries to (a) deploy technological tools that filter obscene content on the basis of lists of key words,[55] and (b) to show warning ads/public service messages to users when searches for such key words were conducted. Further, the Court noted:[56]

- The need for proactive monitoring of the Internet by an independent agency, which could inform relevant law enforcement agencies of any pedophilic or

50 Section 67A of the IT Act sets out the punishment for publishing or transmitting of material containing sexually explicit acts.

51 While revenge porn is not specifically defined penalised, a 2018 judgment of a West Bengal Court in State of West Bengal v. Animesh Boxi (2018) convicted a student under sections 354A, 354C, 354 and 509 of the IPC and Sections 66E, 66C, 67 and 67A of the IT Act for uploading sexually explicit private video of the victim on a pornographic website, without her consent as revenge or not continuing their relationship.

52 Section 67B of the IT Act seeks to comprehensively address child pornography and sexual abuse. This is also addressed via a special law on child porn, namely, The Protection of Children from Sexual Offences (POCSO) Act, 2012.

53 Such offences include for instance, child grooming - see Section 67B of the IT Act, cyberstalking - see Section 354D of the IPC, online sexual harassment - see Section 35A, of the IT Act.

54 This matter was initiated in 2015 in view of child pornpgraphy and rape videos being circulated on communication apps and social media platforms. During the course of hearings (in 2017), the Supreme Court directed the constitution of the Ajay Kumar Committee to make recommendations on how to stop the circulation of such content, while protecting the identity of victims.

55 Search engines were directed to expand the list of key words which may possibly be used by a user to search for pedophilic or rape related content online. The government was directed to work with companies/society organizations to suggest lists of key words that link to pedophilic or rape related content.

56 See order dated 23.10.2017In Re: Prajwala (2015)

rape related content. Law enforcement agencies/relevant government agencies could then take action to block the content by issuing relevant instructions to intermediaries under existing statutory powers;

- The importance of establishing reporting mechanisms, using which the public could make complaints of pedophilic or rape related content, anonymously and easily;
- The need to establish a central agency to maintain and verify the hashes of all known pedophilic and rape related content;
- Need for proactive identification of "rogue sites" by an independent agency and blocking access to them.
- Need for investing in research and development around artificial intelligence, machine learning and deep learning techniques to identify and automatically filter (at the time of upload) pedophilic and rape videos.

More recently, the Madras High Court imposed an interim ban on the popular social media application TikTok, in view of the role it allegedly played in enabling dissemination of sexually explicit and harmful content and exposing children to sexual predators.[57] The ban was lifted pursuant to the platform demonstrating various safety features and adoption of content moderation practices.[58]

In terms of action taken by executive authorities to combat sexually explicit online content, it is key to note that, despite the fact that 'obscenity' is not a ground on which content can be blocked under Section 69A of the IT Act, the government has repeatedly attempted to disable access to obscene or pornographic content, either on its own or in

57 In April 2019, the Court directed the government to ban the TikTok app, due to reported incidents of pornographic content involving children, content with foul language, suicide committed by users, death during taking of selfies, among other things. The order also prohibited the mediafrom telecasting videos made using this application.See order dated 3.04.2019 S. Muthukumar v. The Telecom Regulatory Authority of India (2019)

58 Tik Tok highlighted features such as systems for reporting of objectionable content, efficient and trained content moderation mechanism, parental contro measures to limit the use of the application by children, proactive takedown mechanisms including artificial intelligence powered algorithms that can detect pornographic content etc. See Order dated 24 April 2019S. Muthukumar v. The Telecom Regulatory Authority of India (2019).

pursuance of court orders. Several of these efforts have been via directions to internet service providers.[59]

These attempts are largely sporadic and do not appear to have caused any difference in the volume of obscene content that is accessible online (Singh, 2019).[60] Further, the processes used to block such content continue to lack in rigour. Numerous non-pornographic websites are often caught up in the list of proscribed urls (Prakash, 2016). It also appears that blocking instructions are not enforced uniformly by/across different telecom service providers (Kushagra Singh, Grover & Bansal, 2020).

4.3. Defamatory content

Indian law recognises both civil and criminal remedies for persons aggrieved of defamatory content.[61] While the defamation provisions are regularly used against newspapers and other publishers, increased use of the Internet in general, and social media in particular, has led to the rise of defamation claims against users of online platforms and indeed, platforms themselves.

Judicial developments and regulatory practice

The range of online defamation related suits in India provide an interesting insight into the wide number of issues that are of concern to courts when it comes to the role of intermediaries in relation to the spread of harmful online content. For instance:

- In 'Subodh Gupta v. Herdsceneand' (2019), the Delhi High Court directed the concerned intermediary - Instagram - to provide details of the person/entity

59 Incidents include (a) the directions to ISPs in 2009 to ban a popular toon pornographic website(Shruthijith, 2009); (b) direction to ban 857 pornographic websites (later revised to only websites hosting child porn) (Ghosh, 2015) (c) Subsequently again in 2018 based on a judgment of the Uttarakhand High Court and another by an Additional Chief Metropolitan Magistrate, Mumbai (In Re: In the matter of incidence of gangrape in a boarding school situated in Bhauwala, District Dehradun v. State of Uttarakhand, 2018) and (Internet Freedom Foundation, 2019).

60 Interestingly, reports indicate that the efforts by the government to block access to pornographic content has merely lead to the increased adoption of VPN services to bypass any network restrictions (Singh, 2019).

61 See Sections 499 and 500 of the IPC.

behind the account that posted the allegedly defamatory content. Interestingly, this information was to be provided to the court in a sealed cover.

- In 'Youtube LLC v. Geeta Shroff' (2018), the Court lamented the absence of data localisation laws, that in its opinion, allowed platforms to plead inability to remove illegal content.

- In a case filed by PepsiCo Holdings against a number of social media platforms (Facebook, Twitter, Youtube), the Delhi High Court passed several interim orders mandating the blocking of hundreds of allegedly defamatory videos ('PepsiCo India Holdings Pvt. Ltd. v. Facebook, Inc.' 2018). In addition to the content specifically alleged as defamatory, the court initially also required the platforms to block or remove "any other similar videos". This direction was subsequently suspended. Nevertheless, reports indicate that the directions of the court may have lead to the concerned intermediaries blocking large quantities of content that were not per se defamatory or were simply satirical in nature, that is the end result was overblocking of content (Deep, 2018a) and (Christopher, 2018).[62]

- In 'Swami Ramdev v. Facebook' (2019), the Delhi High Court ordered the platforms concerned to hand over the 'Basic Subscriber Information' related to the allegedly defamatory videos, to enable the plaintiffs to take action against the uploaders of the content. Thereafter, the court, which had initially only required the allegedly defamatory content to be blocked from access in India, extended the scope of its order to require the platforms to block access to the allegedly defamatory content on a global basis i.e. the content should not be viewable by anyone in any jurisdiction. Further, the plaintiff was permitted to request the platforms to take down any offending material directly in case of any future uploads of the allegedly defamatory material. The platforms would however be free to contest such a request, and require the plaintiffs to pursue their remedies under law (Mandhani, 2019).[63]

62 The matter has since been pending hearing as the parties are apparently engaged in talks to settle.
63 This matter is currently pending adjudication in the Supreme Court.

4.4. Seditious or content related to terrorism

Indian laws penalise the publication of content that brings or attempts to bring hatred or contempt or excites or attempts to excite disaffection towards the government.[64] Sedition laws have often been used to prosecute individuals for posting a wide variety of content in the digital space- particularly in the form of social media posts or messages shared via messaging services. For example, action has been taken against users who have:

- Posted content supportive of terrorist or separationist movements;[65]
- Criticised elected officials or the judiciary;[66]
- Posted altered lyrics of the national anthem online.[67]

It appears that sedition related offences are often used to take action against individuals despite the facts of the case not always indicating the presence of the ingredients of the offence (Kovacs & Nayantara, 2017). The potential for misuse of these laws is not helped by the ambiguous nature of some of the phrases used in the relevant sedition and terrorism related laws.[68]

Regulatory developments

We have not come across any cases specifically pertaining to the responsibility of intermediaries with regard to seditious content.[69] However, there are ongoing petitions being heard at various High Courts filed by law enforcement agencies or by individuals seeking to either ban specific applications, such as Telegram, or requiring

64 Refer Section 124A of the IPC. Further, laws such as the Unlawful Activities (Prevention) Act of 1967 and the Prevention of Insults to National Honour Act, 1971 also criminalise certain types of behaviour that threaten national sovereignty, or insult 'national honour'. Other state legislations may also be used to criminalise acts that threaten the state, such as the Maharashtra Control of Organised Crime Act of 1999.

65 See ('Mehdi Masroor Biswas v. State of Karnataka', 2018), ('Arvinder Singh v. State of Punjab', 2018) and ('Kishorchandra Wangkhem v. The District Magistrate, Imphal West Government of Manipur', 2019).

66 See (The Wire Staff, 2019) and (Dahat, 2018).

67 See (Special Correspondent, 2014).

68 In some cases, persons were arrested for allegedly posting "anti-national" content on social media platforms, despite the absence of any law in this respect. We also noted one case - 'Kishorchandra Wangkhem v. The District Magistrate, Imphal West Government of Manipur' (2019) - where an individual was punished with preventive detention - in order to prevent him from accessing social media (though this order was subsequently quashed).

69 See however to the incidents involving sale of goods allegedly violating laws pertaining to India's national emblems, dealt with later on in this paper

intermediaries to implement various technical measures (such as linking user IDs with Aadhaar numbers, building in traceability on platforms, etc.). It appears that law enforcement agencies and government departments are particularly concerned with the use of social media platforms or communication apps to radicalize persons, to encourage them to join terrorist movements or to mobilise in protest against the State.[70]

In general, responses to such concerns involve either (a) the arrest or prosecution of the relevant content uploaders, should their identity be determinable, (b) shutdown of networks to prevent spread of dangerous content,[71] and (c) directing intermediaries to block access to or take down certain content under the IT Act framework.

Media reports indicate that various state agencies also regularly scan social media platforms and other websites to gather intelligence regarding such types of content, including via specially developed sentiment analysis tools.[72] Some law enforcement agencies, such as the Anti-Terror Squad in Maharashtra, have launched efforts to propagate counter-narratives to radicalisation efforts on social media, and to "deradicalise" Indians (Taneja & Shah, 2019).

While no changes to law and policy addressing such types of speech or the role played by intermediaries have been proposed recently, the Government has joined a number of international and multi-stakeholder initiatives intended to tackle the *"terrorist exploitation of the Internet"*. This includes, for instance, the Christchurch call to address terrorist and violent extremist content online (Ministry of Foreign Affairs and Trade, Government of New Zealand, 2019).

70 A long-standing concern is the use of social media to spread inflammatory and viral videos, such as those of brutality by the Indian military, in the state of Jammu and Kashmir. A more recent concern has been the use of social media by the Islamic State to spread their propaganda, to foment communal tensions, to radicalise Indians, or to recruit Indians (Taneja & Shah, 2019) and (Press Trust of India, 2019).

71 For instance, there have been numerous instances of network shutdowns being utilised in the State of Jammu and Kashmir to check the spread of messages on social media that could potentially encourage protests or violence in the region.

72 See, for instance, the use of an "advanced application for social media analytics" by different departments at the Central and State Government to scan, monitor, analyse and categorise social media content as "positive" or "negative" (Shrivastava, 2018). Proposals for the creation of a "social media communication hub" issued by the Ministry of Information and Broadcasting and a social media strategy agency for the UIDAI were also challenged at the Supreme Court. The case was dismissed after the Government withdrew the notification for the proposal (Jalan, 2019a) and (Press Trust of India, 2018b).

4.5. Content that interferes with democratic processes and institutions

Various laws in India are aimed at checking abuse of processes that are central to the functioning of India's democratic institutions. This includes:

- **Restrictions on the sharing of electorally sensitive material:** India's electoral laws allow restrictions to be imposed on the circulation of material by candidates in various circumstances - notably, in the 48 hours preceding voting.[73] A major concern for the Election Commission of India has therefore been the ability to enforce such restrictions in the online context.

- **Contempt of court:** The Contempt of Courts Act, 1971 contains civil and criminal penalties for publishing content that lowers the authority of the court, interferes with any judicial proceeding or with the administration of justice. There are a number of cases of users being proceeded against for posting comments on social media that were critical of the judiciary.[74] While we did not find a case where an intermediary was proceeded against for a contemptuous act, courts have, however, directed intermediaries to take down offending content and provide them with information regarding the identities of users who upload or re-upload content.[75] In one case, the Himachal Pradesh High Court directed the deletion of a contemnor's Facebook account, and sought to restrict him from operating WhatsApp or other forms of social media, so that he could not post "directly or indirectly any scurrilous, offensive, intimidatory or malicious posts against any individual(s) or institution(s)" (Vishwanath, 2018). It is unclear if and how the intermediaries concerned are expected to restrict the contemnor from creating new accounts on their services.

73 See Section 126 of the Representation of People Act, 1951.

74 This has lead to some commentators questioning whether contempt laws in the country need to be re-examined given their potential to curb free speech (Bhatnagar, 2017), (Wire Staff, 2016) and (Board, 2019).

75 See, for instance,Court in its own motion v. S Gurumurthy (2018). Note that the Contempt of Courts Act specifically excludes the innocent distribution of contemptuous content.

Judicial developments and regulatory practice

Most of the judicial and regulatory developments on this issue have concentrated on the distribution of electorally sensitive material on the Internet.

In 2018 the Election Commission of India (ECI) constituted a Committee under the chairmanship of a Deputy Election Commissioner to suggest a ways to address issues pertaining to the use of social media during political campaigning periods amongst other concerns (Election Commission of India, 2019b). The ECI has thereafter sought to implement various measures to address the issue. For instance, it has established a system of "social media experts" to assist its Media Certification and Monitoring Committee in tracking and raising specific items of problematic claims being made by political parties (Election Commission of India, 2019a).

The ECI is also working with prominent social media platforms to bring the recommendations of the above Committee into force. In March 2019, social media platforms, under the aegis of the Internet and Mobile Association of Indian (IAMAI), submitted a "Voluntary Code of Ethics for the General Election 2019" that sought to set out certain commitments to be adopted by them from 20th March 2019 for the duration of the 2019 general elections in order to "*increase confidence in the electoral process*" (Internet and Mobile Association of India, 2019).

In the context of political advertising and sharing of electorally sensitive material on social media, the ECI has taken several steps to enforce existing campaigning restrictions on online media. As early as 2013 the ECI had issued instructions to electoral officers and political parties on the use of social media, defined as including collaborative projects (like Wikipedia), blogs and microblogs (like Twitter), content communities (Youtube), social networking platforms, and virtual game- worlds (like "Apps") (Election Commission of India, 2013). Amongst these requirements was the need for candidates to follow the model code of conduct for online content, as well as pre-certifying advertisements, that would apply *mutatis mutandis*. These were renewed for the 2019 elections as well (Election Commission of India, 2018).

4.6. Content that infringes intellectual property rights

A number of statutes recognise and regulate different types of intellectual property (IP) rights in India.[76] Statute recognises specific criminal offences and provides penalties for infringements.[77]

The issue of online piracy and sale of counterfeit goods is one that has prompted significant regulatory attention in India.[78] India is often considered a hot-bed of online IP infringements and rights holders have not been shy of approaching courts.[79] This area has therefore seen significant development in terms of providing a body of law to refer to in the context of intermediary regulation.

Judicial developments and regulatory practice

The Copyright Act was amended in 2008 to include a specific "safe harbour" for online intermediaries.[80] A 2017 decision of the Delhi High Court in 'Myspace Inc. v. Super Cassettes Industries Ltd.' (2017) explains how this "safe harbour" works.

Here, the Court held that an intermediary would only be deemed to possess knowledge about an infringement on its platform, after the rights holder was able to "*give a detailed description of its specific works which are infringed to enable the web host to identify them*". The Court thus placed the onus of bringing infringements to the attention of intermediaries on the rights holders themselves. A key reason for this was to

76 Refer to the Copyright Act of 1957, the Trade Marks Act of 1999, the Design Act of 2000 and the Patents Act of 1970. In addition, relevant common law doctrines, such as passing-off, are recognised in India as well.

77 For instance, the Copyright Act of 1957 prescribes criminal sanctions for several offences, including the intentional infringement of rights conferred by the Act (Section 63), the use of pirated computer programmes (Section 63B), the circumvention of digital rights management technologies (Section 65A), etc.

78 See, for instance, the National Intellectual Property Rights Policy of 2016 notes the need to check online counterfeit trade and digital piracy via different measures, including technological solutions.('National Intellectual Property Rights Policy', 2016).

79 A number of industry reports from 2009 onwards from film, music or software industry associations have consistently claimed that India is amongst the top ten countries in the world for online piracy(Mohan, 2009), (Deloitte and Indian Music Industry, 2019) and (L. Jha, 2019). Scholars have however questioned the accuracy of such claims (Scaria, 2013).

80 This is contained in Section 52(1). Rule 75 of the Copyright Rules of 2013 define a specific notice-and-takedown regime for rightsholders in this regard.

ensure that intermediaries do not act as "private censorship regimes".[81] The Court did however, direct MySpace to keep detailed accounts of take-down requests.[82]

Several aspects of the Court's reasoning are noteworthy. First, the court observed that online platforms cannot be expected to adhere to the same standard of knowledge as would be applicable in the case of copyright infringement in a physical context. Such a requirement would mean that platforms would have to scrutinise all content shared via their service, which would be unfeasible. Second, the court noted that, the use of automated means to affect the infringing content (say by inserting advertisements into a video), would not cross the "actual knowledge" threshold. Human intervention by Myspace would be required in order to attribute knowledge to the platform.[83] Third, the court held that platforms could not be expected to run a general filter and take down allegedly infringing content on the mere notification of a rights holder, as this could affect users relying on the various exemptions to copyright law - such as fair use. A requirement for general monitoring and filtering content could therefore "*snuff out creativity*". The court was therefore clear in holding that it could not direct ex-ante screening of uploaded content for IP infringement, in view of the possible costs to the platform and the chilling effects on civil liberties.

This position was reaffirmed in 'Kent RO Ltd. v. Amit Kotak' (2017), where the court was hearing complaints filed under the Design Act, 2000. Once again, the Delhi High Court noted that the IT Act and the rules thereunder did not require intermediaries to introduce filtering tools.[84]

81 Specifically, the court noted that "if an intermediary is tasked with the responsibility of identifying infringing content from non-infringing one, it could have a chilling effect on free speech...such kind of unwarranted private censorship would go beyond the ethos of established free speech regimes" ('Myspace Inc. v. Super Cassettes Industries Ltd.' 2017).

82 The Court directed MySpace to keep an account of all such take-downs, as well as keep details such as the number of viewings of infringing content till its removal, or the advertising revenue earned by it from such content. This was for the purposes of enabling the calculation of damages at the trial stage.

83 The Court notes that *"...knowledge is to be therefore placed in pragmatically in the context of someone's awareness (i.e a human agency); a modification on the technical side by use of software would per se not constitute knowledge. Nevertheless, if the software requires some kind of approval or authorization from a person or authority as opposed to a computer system then knowledge can be attributed. This however has to be seen at the stage of trial..." '*. Refer paragraphs 36 and 37, ('Myspace Inc. v. Super Cassettes Industries Ltd.' 2017).

84 The Court also specifically stated that the doctrine of "auto block" laid down in Sabu Mathew George v. Union of India (2017) was in the context of the PNDT Act of 1994 and not under the IT Act or Rules - clearly intending to delineate the scope of his observations on the use of filtering tools to just this framework.

As far as cases pertaining to trademark infringements are concerned, a number of cases have dealt with the issue of whether the practice of providing trademarked keword suggestions, to competitors of the rights holder, by search engines was illegal. The Madras High Court in 'Consim Info Pvt. Ltd. v. Google India Pvt. Ltd.' (2013) held that search engines can be held liable in cases "*where a completely arbitrary or fanciful name, which has no nexus or connection with the nature of the goods or services, is adopted as a trademark*".

A number of recent cases at the Delhi High Court, starting with 'Christian Louboutin SAS v. Nakul Bajaj' (2018), have now started to lay down clear principles to delineate situations where and when online platforms (e-commerce marketplaces in particular) can claim the benefit of safe harbour. These principles seek to examine whether the platform can be considered an "active participant" in the illegal transaction, based on factors such as the type of functions performed by the platform, the range of service offered by them to sellers, etc.[85]

A similar approach was used by the Court in 'Luxottica Group S.P.A. v. Mify Solutions Pvt. Ltd.' (2018). Here, the Court held that the platform would not recieve the benefit of safe harbour as:

- its policies simultaneously guaranteed the authenticity of products on its platform while also claiming that it was merely a facilitator of sales;
- it was not meeting its due diligence requirements under Section 79;
- it was handling the shipping of the counterfeited products.

The platform was therefore seen as actively participating in the commission of an offence and therefore could be proceeded against together with the actual sellers of the (illegal) products.

85 In this case, the court listed a number of factors that could be considered, including: (1) whether the platform performed any of twenty one specific tasks with relation to the product such as whether they are involved with packaging the goods or providing inventory storage space to sellers, etc. and (2) the policies in place to restrict infringements.

In 'Amway India Enterprises Pvt. Ltd. v. 1MG Technologies Pvt. Ltd.' (2019), the Court held that safe harbour could not be claimed by an e-commerce platform if:

- it did not strictly observe and adhere to its own internal policies
- it did not demonstrably comply with the due diligence requirements under the Intermediary Guidelines, 2011
- it did not take measures to ensure that it was not inducing breach of third party contracts, once notified of the same.[86]

While the courts in the above matters have indeed put in place relatively sound principles to determine whether a platform is actively contributing to the breach of IP laws, the scope of some of the directions issued by courts does give some cause for concern.

For instance, Delhi High Court has directed marketplaces to notify a rights-holder of products carrying its marks when they are being uploaded and then to obtain the latter's concurrence before offering such products for sale ('Christian Louboutin SAS v. Nakul Bajaj', 2018). Further, marketplaces must obtain a certificate of genuineness from its sellers, and must not list any products of any sellers who are unable to provide such guarantees on its platform.

Interestingly, the draft National E-Commerce Policy, 2018, which seeks to regulate the functioning of electronic commerce martkeplaces practically replicates several of the directions from the Delhi High Court in the above cases. This is problematic, since it extends case-specific directions to all marketplaces, which could be impractical to follow in view of the possible differences between business models used by platforms.

86 Examining the role played by the platforms in enabling the breach of exclusive disribution agreements signed by online sellers with third parties, the court noted that the platforms were providing a "refuge" for sellers to breach their contracts including by assisting sellers in packaging and shipping products and by enabling the registration of their warehouses as the seller's 'place of business' thereby enabling the sellers to claim tax credits. The court also repeatedly emphasised that the internal policies of marketplaces cannot be mere "paper policies", but must be enforced ('Amway India Enterprises Pvt. Ltd. v. 1MG Technologies Pvt. Ltd.' 2019).

4.7. Sale and advertisement of regulated goods and services

Several Indian laws restrict, regulate or prohibit the sale, distribution or promotion of different products and services, primarily on grounds of public health, safety and morality. The increasing use of the Internet has resulted in numerous online platforms and websites being used to advertise or sell such products and services, often bypassing the restrictions that would otherwise apply to their sale in the physical world. Courts and regulators have had to contend with online sale and promotion of a range of regulated products and services - from narcotics to prenatal sex determination kits, sex-toys, firearms and various chemicals.

In general, intermediaries tend to play three roles as far as the sale of regulated goods and services is concerned - (a) they can carry user generated content that advertises the sale of prohibited goods or services, (b) they may allow users to directly buy products or services from sellers on their platforms, or (c) they may provide delivery and similar services to connect buyers to offline sellers or provide other services in relation to an offline trade such as warehousing, invoicing etc.

Judicial developments and regulatory practice

Generally, regulators and courts have focused on blocking content that is seen as promoting the sale of regulated goods and services. This can be seen for instance, in the context of platforms that carry third party advertising - say pertaining to escort services.[87] The government has from time to time ordered the blocking of various websites that carry such content, for instance, by ordering the blocking of 240 websites in June 2016

87 The Mumbai High Court has had occasion to examine the matter in a public interest litigation filed before it in early 2016. Upon direction, the police pointed out that they had obtained an order from a magistrate's court to delete or block 316 websites that were advertising escort services. They had then forwarded a list of 174 websites to the relevant central government department to take necessary action (i.e. issue blocking instructions to the domain registrar - in this case godaddy.com) (Press Trust of India, 2016b) and (HT Correspondent, 2016a). In subsequent hearings of this matter it appears that the Court was not impressed by the investigative and remedial action taken by the police.

(on the recommendations of a committee established under the Ministry of Home Affairs) (Prakash, 2016) and (Press Trust of India, 2016a).

That said, it appears that government officials have also recognised the problems with attempting to deal with online content in such a manner - not only is the scope of the problem large in terms of the number of such advertisements, the ease of replicating and re-uploading content means the relevant authorities are always on the backfoot (Press Trust of India, 2016a).[88]

In the context of sale of products such as narcotics, alcohol and tobacco products, much regulatory attention has focused on cracking down on the platforms providing such services.[89] Interestingly, it has been reported that the Excise Department in Maharashtra, has apparently directed telecom and internet service providers "to monitor their clients to check if anyone is indulging in illegal online or on-call delivery", and is working with the cyber police to track offenders (Tembhekar, 2018b).

In some cases, the Government has sought to change existing rules to ensure they can apply to the Internet. For instance, the Prevention of Cruelty to Animals (Pet Shop) Rules, 2018, were recently revised to ensure that online platforms either register as "pet shops" (if carrying on the sale themselves) or ensure appropriate registration of users posting advertisements for sale of animals, etc (Mantri, 2018).

Another important issues addressed in this context is pertaining to the advertisement of pre natal sex selection services. In Sabu Mathew George v. Union of India (2017), three search engines (run by Google, Yahoo and Microsoft) were alleged to be listing/ carrying advertisements and other information in contravention of the Pre Conception and Pre Natal Diagnostic Techniques Act, 1994 (PCPNDT). Backed by the stance taken

88 As an aside, it is also interesting to note that as in the case with the June 2016 blocking requests, the list of websites/ urls for blocking is often improperly curated (for instance it may include multiple listings of the same url, wrong urls, entire domains rather than specific pages, and may also include non-violating websites). Further, the government often does not release the list in public leading to a lack of transparency in the matter (Prakash, 2016).

89 In 2015 the Delhi government was amongst the first to begin restricting the use of the Internet for alcohol distribution services (Press Trust of India, 2015) Other states to have taken action against online alcohol delivery and sales include Maharashtra, Punjab and Karnataka (Tembhekar, 2018a), (HT Correspondent, 2016b), (Aiyappa, 2018) and (Deep, 2018b).

by the government, which encouraged intermediaries to automatically block illegal content, the Supreme Court in a series of orders, held that:

- Intermediaries are under an obligation to see that the "doctrine of auto block" is applied to illegal content, within a reasonable period of time. Search engines should act to pre-emptively block access to content that contained a list of 42 phrases/ words that were associated with the practice of pre-natal sex determination.
- That it was difficult to accept that intermediaries would only act once illegal content was brought to their notice. Intermediaries must work to find an appropriate solution and comply with existing laws of the land. The court would not make specific recommendations in this regard, but would leave it to the intermediary concerned to take appropriate action.
- That the central government should constitute a nodal agency to act as a body to educate the public and liaise with intermediaries to ensure takedown of illegal content. Specifically, the agency is to request information from the public regarding content that violates the PCPNDT and notify the intermediary concerned. The intermediary is then required to take down such information within 36 hours and notify the agency of the action taken. The agency is then to publish a list of action taken on its website.
- That intermediaries must adopt an in-house procedure (involving the appointment of experts) to identify and remove content that violates the letter and spirit of the PCPNDT. In case of doubt regarding the legality of any content, the intermediaries should liaise with the nodal agency established by the central government.

In accordance with the court's orders, it appears that the three intermediaries involved have indeed appointed in-house experts on the issue. They have also made declarations to the court that they will not permit content that breaches the law to be made available on their websites and will abide by decisions of the nodal agency to block content (Sabu Mathew George v. Union of India, 2017).

This case appears to indicate the willingness of courts to cast greater obligations on intermediaries to screen their content for advertisements and other material that violates the law of the land, atleast in the context of offences that are seen as having wide social

impact. Notably, no such orders have been passed in the context of sale of narcotics, alcohol, or indeed advertisement of escort services.

One can also see attempts at inducing greater coordination and cooperation between intermediaries and governmental/regulatory agencies to deal with sale/advertising of regulated goods and services online.

4.8. Emerging harms

In this section we explore some of the new types of online harms involving intermediaries that have come up in the global discourse and their relevance in the Indian context. These harms may not be specifically covered under any existing laws.

4.8.1. Disinformation and fake news

An increasingly important issue for policy makers, both globally and in India, is the challenge of "fake news".[90] A review of literature suggests some consensus that "fake news" should be used to refer to content that portrays false or misleading information as authoritative and reliable news stories [91] While we have discussed the issue of rumours spreading via messaging services in previous sections, here, we concentrate on the broader concern of the spread of falsified information that mimics news content.

Literature links the increasing use of social media and messaging services as primary news sources, with the rise of fake news in the media overall (Allcott & Gentzkow, 2017), (UNESCO, 2018) and (Caplan, Hanson & Donovan, 2018). The presence of such services has made it easy to rapidly create, spread and amplify false or distorted information at scale with relative anonymity, through automated tools, and without

90 The term itself lacks precise meaning. Scholars point to two basic interpretations of the phrase: (1) when understood as a "genre", it refers to the deliberate creation of "*pseudojournalistic disinformation*", and (2) when used as a "label", it becomes a term used to "*delegitimize news media*", or more generally, to discredit disagreeable reportage, ideas or authorship as being "fake", rather than engage with such work on merits (Egelhofer & Lecheler, 2019).

91 For instance, one definition is *"fabricated information that mimics news media content in form but not in organisational process or intent*". See (Lazar et al., 2018).

incurring large costs. The motivations of the actors behind such efforts are wide-ranging - from purely financial interests to deliberate attempts to weaken public trust in institutions and experts to attempts to influence the outcomes of elections. The increasing incidence of such content online has been linked to a diverse and complex range of harms and worrying trends, such as an increase in "*junk science*" or in divisive political propaganda designed to "*undermine democracy*" (Hopf, Krief, Mehta & Matlin, 2019) and (Morgan, 2018).

India has been specifically noted as a hotbed of fake news, with recent studies showing that Indians are regularly exposed to large quantities of fake news online.[92] We have found reporting of 'fake news' in multiple contexts - for example, pertaining to medical misinformation;[93] price-sensitive false information;[94] and, political propaganda.[95]

There is no specific legislation that proscribes "fake news" when understood in many of these contexts. However, there have been several attempts by the government to tackle the issue. For instance, the 16th Parliamentary Standing Committee on Information Technology in February 2019 has sought the views of both the government (the Ministry of Electronics and IT) and Twitter on the subject of *"safeguarding citizen's rights on social/online news media platforms*".[96]

92 For instance, a recent study by Microsoft found that, out of 22 countries' Internet users surveyed, Indians reported the most amount of fake news (Microsoft News Center India, 2019). Another study by the Reuters Institute found that Indian online news users were particularly worried about encountering false news, hyperpartisan content and poor journalism online (Aneez, Neyazi, Kalogeropoulos & Nielsen, 2019). The fact that a number of fact-checking services, such as AltNews or BOOM, have gained popularity in India is also a useful indicator of the rise of the challenge.

93 There are multiple instances being noted of messages on social media and messaging services being circulated that offer false and inaccurate medical advice, or contain unverified health myths and misleading claims around, *inter alia,* vaccines, sanitary napkins, biopsies, and even cancer and other terminal illnesses.

94 "Multiple companies have complained that "fake news" have caused them significant monetary damage. In one case, a jewellery business moved the Kerala HC seeking the regulation of social media companies after it lost more than $ 70 million in revenue after a fake message was shared on WhatsApp that it was using counterfeit gold. In another, an e-commerce company claimed that it lost 71% of its market value on a single day, after a WhatsApp message was shared amongst stock-traders that posed ostensibly misleading concerns about its accounting practices.

95 A recent study focusing on data collected from Facebook and WhatsApp in the months leading up to the 2019 general election found that "junk news" (defined therein to include disinformation and political propaganda posing as news) and "misinformation" was spread widely during that time period by pages and groups affiliated with political parties or by supporters of political parties, though the study did not seek to draw any conclusions as to whether these had any impact on electoral outcomes(Narayanan et al., 2019). Other studies have utilised consumer surveys to state that social media may not have had a significant impact on electoral outcomes, since a large percentage of India's electoral base still relies on traditional news media sources(Centre for the Study of Developing Societies, 2019).

96 This issue is expected to be taken up by the 17th Committee as its first item of business.

Within the executive, one of the earliest actions, was in April 2018, when a draft order was released by the Ministry of Information and Broadcasting (MIB) that would have permitted it to withdraw the accreditation of journalists accused of publishing fake news. This was quickly withdrawn (Pahwa, 2018). Later, an interministerial committee was appointed in 2018 by the Prime Minister's Office under the Ministry of Electronics and Information Technology (MEITY) to examine issues such as fake news, malicious online content as well as digital broadcasting, amongst other concerns.[97]

The Press Council of India has also taken cognisance of this issue, by issuing warnings and attempting to put forward a formal definition of fake news.[98] Two identical private members' bills have also been suggested to specifically tackle "fake news", which have prescribed heavy penalties and fines.

Some regulators have also picked up the matter within their specific domains. For instance, SEBI has examined the issue of false price sensitive information being circulated as a potential form of unfair market conduct.[99] The Election Commission of India has also sought to pursue criminal actions in relation to "fake news".[100]

4.8.2. Bias, discrimination and lack of transparency in platform practices

Another problem that has attracted the attention of regulators across jurisdictions is the possibility of platforms acting in biased and discriminatory ways when implementing their internal policies and practices.

97 There is no information available on the outcome of this process.(A. N. Dutta, 2018).

98 The definition proposed considers "fake news" as simply 'falsified' news.

99 See the report of the Committee on Fair Market Conduct, that suggested that the regulations on fraudulent and unfair trade practices should be amended to extend provisions on the publication of misleading advertisements to include "*information disseminated through any physical or digital means including the Internet*", and further, that the provision on the planting of false news should also be similarly extend, and that such planting would be deemed a fraud, if done with the objective of impacting the price or volume of a security. The Committee's recommendations on the regulations were brought into force as of February 2019

100 News reports in February 2019 indicate how the ECI submitted a complaint to the Delhi Police to institute a case under Sections 505(1)(b), 463, 471 of the IPC and Section 3 of the State Emblem of India(Prohibition of Improper Use) Act, 2005regarding the circulation of false messages on WhatsApp regarding NRIs having a facility to vote online for the 2019 election (Reporter, 2019).

Social media platforms, in particular, have come under fire (in India as with other jurisdictions) for allegedly favouring certain political ideologies in their content curation and moderation practices.[101]

In India, this issue has reached the highest levels of government - allegations from right-wing groups of biased content moderation practices were amongst the developments that prompted the Parliamentary Committee on Information Technology to summon representatives from Twitter, Facebook, Whatsapp and Instagram to discuss the topic of "safeguarding citizens' rights online in India" (Soni, 2019). In particular, the utilisation of algorithmic content moderation systems has been cited by a member of parliament as the mechanism through which such bias plays out, by filtering, curating and amplifying content in ways that favour specific political viewpoints and ideologies.[102]

A second type of allegedly discriminatory practice concerns the manner in which actions are taken against users in order to implement internal content moderation policies. An ongoing case before the Delhi High Court involving Twitter has brought this into focus. The petitioner is seeking to challenge the platform's decision to ban his user account on the ground that his right to speech has been compromised. His petition also calls for regulatory guidelines to be issued in this regard by the Ministry of Electronics and Information Technology, citing a failure of the self-regulatory practices being followed by such platforms (Barik, 2020).[103]

There is growing evidence that the application of content moderation and conduct rules by platforms can often result in inconsistent and arbitrary outcomes, that to some extent can be based on the level or nature of public outcry over any particular incident. For instance, the TOSsed Out project of the Electronic Frontier Foundation focuses on demonstrating that content moderation rules and conduct rules have a a

101 A notable example comes from the Trump administration, which has raised concerns of an "anti-conservative" bias on platforms like Facebook, Google's YouTube and Twitter. This led to the creation of an online form by the White House allowing individuals to report incidents of censorship experienced by them on social media sites (Associated Press, 2019). Similar accusations have been levelled against various social media companies in India (Mehta, 2019).

102 The member of parliament has called for regulation to hold social media platforms accoutable for this form of *algorithmic bias* (Tripathi, 2019).

103 The Court had issued notice to both Twitter and to the Ministry.

disproportionate impact on groups who do not have easily access to other mediums of communication (Electronic Frontier Foundation, 2019).[104]

Apart from social media platforms, e-commerce marketplaces (such as Flipkart and Amazon) have also had to contend with allegations of biased and discriminatory practices. This has gained some regulatory attention - allegations that marketplaces favour the products of companies they have a stake in, has promoted changes to India's foreign direct investment policy, and also found place in the Draft E-commerce Policy.[105]

At the heart of these concerns is the issue of platform accountability and transparency. This is, at least in the context of the use of automated tools, being sought to be (partially) addressed through provisions relating to automated decision-making in data protection laws (such as the European General Data Protection Regulation). The possibility of unfair, biased, or discriminatory results being generated through automated processes is also one of the motivations behind the proposed law on algorithmic accountability that has been introduced in the United States. Various jurisdictions such as Germany and the UK are also looking to implement procedural regulations that seek to ensure some level of consistency in decision making by platforms.

4.8.3. Internet addiction

Another possible online harm meriting more detailed examination is the issue of Internet addiction, particularly amongst children. As per media reports, prominent medical colleges are seeing a rise in the number of complaints in this regard.[106]

Research conducted by the National Institute of Mental Health and Neuro Sciences of 1763 medical college students noted the possibility of a positive correlation with

104 News reports indicate how such concerns may play out in the Indian context as well. For instance, members of minority communities have alleged that Twitter has a bias against them when it verifies accounts to permit the use of "blue ticks" (F. Jha & Taskin, 2019).

105 These have been brought up as concerns of competition law and fair market practice and are currently under consideration by the Competition Commission of India.

106 For instance, the Behavioural Addiction Clinic has noted that complaints of Internet addiction have doubled in the last two years (Press Trust of India, 2018a). NIMHANS registered its first case of Netflix addiction in India in 2018, taking in a man who was spending over 7 hours a day over 6 six months on the platform (Ganjoo, 2019).

psychological distress, particularly depression, and Internet addiction, and that *"the two may co-exist and exacerbate each other"* (Anand et al., 2018). The researchers suggested the screening of medical students for psychological distress and Internet addiction and to create awareness around the issue amongst students and faculty. While such individual cases and studies are useful in understanding the impact of Internet usage in India in isolated scenarios, more research will be required in India to conclusively determine the extent to which internet addiction is a concern.

While we did not find cases or regulatory developments examining this issue in depth, the concern of Internet addiction has been raised in some specific contexts, such as petitions being filed before the courts to ban video games[107] and online poker and gambling websites.[108]

5. Analysing the evolving regulatory approach to online harms

In this section, we analyse the responses of courts and regulators to the online harms examined in the previous section. We examine trends in the application of existing laws concerning intermediaries, and analyse what this could mean for the future of intermediary liability regulation in the country.

5.1. The challenges with a "one-size-fits-all" approach

As discussed in Section 3, certain types or classes of platforms have attracted the focus of regulatory attention in the context of various specific online harms. As argued in previous sections and elsewhere,[109] a clear case exists for a calibrated approach to regulating different types of intermediaries. However, at a global level, there exists no

107 One notable example is the petitions and other efforts aimed at banning the PlayerUnknown's Battlegrounds (Bureau, 2019). The interim ban imposed on TikTok app also cited addiction as a reason(S. Muthukumar v. The Telecom Regulatory Authority of India, 2019).

108 A petition filed before the Delhi High Court has sought to ban online gambling and betting websites for numerous reasons, one of which is their addictiveness (Jalan, 2019b).

109 See (Bailey, Parsheera & Rahman, 2018).

consensus on how the wide variety of intermediaries and their services can be classified and how specific obligations may be imposed based on such classification. Part of the reason is the changing nature of intermediaries, the services they provide, and the functions they perform across the Internet ecosystem.[110] Classifying these services neatly to frame appropriate definitions will be a significant challenge.

In this scenario, the lack of clarity in the IT Act framework regarding the possibility of application of differential obligations is a matter of concern.[111] The only place in the IT Act where different types of intermediaries are (implicitly) differentiated is in the Section 79(2), where there is recognition of a functional differentiation between "mere conduits" and other intermediaries. However, this section, too, does not specifically empower the government to lay down differential regulations for specific types of intermediaries (though equally, it does not prohibit the same). While the government has indeed notified specific guidelines for "cyber cafes", and orders and advisories have been issued to specific types of intermediaries in different contexts,[112] it may be preferable to outline, through statutory means, the ability to regulate specific classes of intermediaries. Notably, the draft e-Commerce Policy, 2019, attempts to classify various types of intermediaries, though an exact definition of categories continues to be missing. The policy seeks to impose certain general obligations on "platforms" and "intermediaries", and also impose differential obligations on specific types of intermediaries such as "marketplaces", "search engines" and "payment gateways".

Going forward, defining these specific terms - representing the most commonly seen platforms - would be necessary to impose suitable and narrowly-tailored obligations.

110 Multiple intermediaries in today's context operate a wide variety of services as integrated or connected services, often as combined offerings to users. Some large platforms are particularly complex entities, offering social networks, news aggregation services, application stores, communication services, e-commerce services, advertising services, payment services or search engines under the same brand or organisation. These can also be offered to both end-users as well as other commercial and corporate entities.

111 We note that as in the case of the draft Intermediary Guidelines 2018, even where the intent of the government has been to impose obligations on a specific category of intermediaries - social media services - the draft use utilise the generic framing, thereby applying the rules horizontally to all categories of intermediaries.

112 See, for instance, the order issued to ISPs operating cable landing gateway stations to adopt a filtering mechanism for child sexual abuse material (Government of India, 2017).

5.2. Self-regulatory processes under Section 79

The text of Section 79 (and any rules issued thereunder) may also need revision or clarification to address an issue that has arisen frequently across the different harms studied in the previous section - that of the scope of self-regulatory processes adopted by intermediaries.

At present, the intermediary liability framework under Section 79 has very basic requirements for self regulation by intermediaries. Intermediaries are required to provide notice, via suitable terms and policies, to users not to undertake various illegal and harmful activities, and to warn them of the possibility that violation of such terms or policies may result in withdrawal of services.[113]

Our analysis indicates that major intermediaries do have in place fairly voluminous policies regarding the types of content that users are restricted from posting on their platforms and the consequences for the same.[114] In general, these policies mirror or draw from legal requirements but they are also shaped by the intermediary's perceptions of what may be deemed as appropriate content by government agencies and advertisers and as per the sensibilities of their users (Bailey, Parsheera & Rahman, 2018).[115] Further, the global nature of many online businesses implies that policies that are framed to comply with the laws of one country may be made universally made applicable to other regions.[116]

Most major platforms in India implement voluntary initiatives which provide some means for users to report content that violates their terms of service.[117] All the

113 See Rule 3 of the Intermediary Guidelines of 2011.

114 For our analysis, we studied terms of use of popular social media companies ShareChat, TikTok, Facebook and YouTube, e-commerce platforms - Amazon and Flipkart, advertising portal - Olx, review site - Mouthshut, and communication platforms - WhatsApp and Telegram.

115 Analysis of the terms of service of popular social media platforms indicates that the kinds of proscribed content or behaviour are extensive ranging from harmful and hateful speech, harm to minors, violent and criminal content, violating intellectual property and privacy rights, and fraudulent content.

116 For instance, Facebook's community standards state that give the "borderless nature" of the Facebook community, the company prohibits the transfer of firearms on its platform, even if this is not barred in a particular country.

117 While nearly all the platforms allow user's to contact them online (through forms or email addresses), some (particularly those based in India) also provide details of grievance officers.

intermediaries reserve their rights to remove or block access to content at their discretion, though they also clarify that they are under no obligation to do so. The terms of service generally indicate that the severity of the action taken would vary depending on various factors, such as the repeated nature of the violation, its likely consequences and the targeting of vulnerable groups, such as minors.[118] The processes for blocking users and/or content (in terms of the mechanisms followed and the standards applied) are not always clearly laid out - though most platforms allow a party affected by a wrongful take-down to approach the platform for redress. The lack of clarity in this regard can make it difficult for users to understand why punitive action is taken in any particular instance.

This problem is exacerbated as the broad and often ambiguous framing of these voluntary policies provide the platforms with a great deal of discretion in regulating user behaviour.[119] This coupled with lack of transparency by intermediaries can lead to problems of censorship of legitimate speech or discriminatory behaviour by intermediaries.[120] This also permits platforms to acquiesce to public concerns or government requests that may also go beyond the explicit terms of the law. An associated problem with the long list of proscribed content is that this may often not be understandable or properly accessible to users. The policies we studied often go into multiple pages and are generally written in legal language.

Notably, as discussed in the previous sections, courts have repeatedly pointed to (a) the need for platforms to have in place appropriate terms and conditions or content moderation policies, (b) to act consistently and speedily on those policies, including by

118 The actions taken may include take down of the specific content, demonetisation thereof, blocking of the user's account (permanently or temporarily) or, in some cases, less severe consequences like flagging the content or marking it as unsuitable for children. In some cases, the policies also suggest that the company will take into account the context of the content, for instance, whether it is artistic, satirical or scientific in nature, while deciding on the appropriate action.

119 For example, TikTok prohibits any content *that"could cause physical, emotional, financial or legal harm",* ShareChat prohibits content that could *"create a hostile environment for other user".* Similarly, WhatsApp also uses fairly broad terminology to describe prohibited activities under their internal policies. Notably, its policy states that any content that *"instigates conduct that is illegal or inappropriate"* is barred by the platform.

120 Examples of this include reported instances of YouTube taking down videos of Syrian atrocities due to its algorithmic inability to distinguish between the propaganda content and legitimate news reporting(Keller, 2018). Similarly, Facebook recieved flak for censoring legitimate posts related to Kashmir(Doshi, 2016).

taking appropriate technical measures to give effect thereto. Literature also demonstrates the scope for arbitrary and inconsistent application of content moderation policies by specific platforms, as well as the opacity of content moderation practices.[121]

In light of the abovementioned concerns, any proposed regulation may need to lay down procedural requirements aimed at ensuring transparency and accountability in the implementation of terms and conditions of intermediaries. For instance, content moderation policies must provide a clear path to raise complaints, ensure appropriate time-lines, reasoned responses, appeals, etc. Intermediaries must also be required to publish sufficiently granular reports at periodic intervals, to enable the public at large and policy makers greater insight into content moderation practices.

5.3. Pro-active monitoring under Section 79

One of the crucial issues that has arisen in the context of preventing online harms is the need for proactive monitoring or filtering of user content by an intermediary.

In this context, the Supreme Court has clarified that an intermediary can only be required to take down content after either receiving a court order or on receiving a lawful notification from the appropriate Government agency.[122] Along the same lines, two cases from the Delhi High Court ('Myspace Inc. v. Super Cassettes Industries Ltd.' (2017) and in 'Kent RO Ltd. v. Amit Kotak' (2017)) note that intermediaries cannot be expected to screen for illegal content on a real-time basis (at least in the context of IP violations).[123]

121 As an example, see (Alice Witt & Higgins, 2019), which examines the moderation of images depicting female forms on Instagram across 4944 images and notes an overall trend of inconsistent moderation. The article finds for instance, that over 22 percent of images removed did not actually appear to violate the platform's content policies.

122 The Supreme Court based its reasoning in *Shreya Singhal* on two factors: (a) that, due to the scale of online content, intermediaries would be in an impractical position if forced have to judge the legality of each piece of content, and (b) that the statute itself did not envisage the intermediary applying its mind in the context of what content to take-down.

123 In the latter case, the court provided several relevant reasons for this, such as noting that there is no provision of law requiring owners of immoveable property or publishers of newspapers or magazines to keep vigilance that the contents of their ads do not violate IP rights, and that such screening requirements would be "*an unreasonable interference with the rights of the intermediary to carry on its business*".

However, in Sabu Mathew George v. Union of India (2017), a "doctrine of auto-block" was adopted to require search engines to pre-emptively block access to advertisements for pre-natal sex determination on the basis of lists of key words. This effectively: (1) creates an alternative way to deem that intermediaries receive "actual knowledge", not in the form of individual orders for individual pieces of content, but by providing a single order with a list of key-words that would operate on a standing basis; and (2) creates an implicit pre-screening requirement, by requiring intermediaries to "pro-actively" scan for content that maps against these key-words.[124]

Similar suggestions have also been seen in:

- The Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications (2017), wherein the Madras High Court directed intermediaries to undertake 'due diligence' to remove all relevant links and hashtags being circulated on the Internet regarding the Blue Whale game.
- 'Christian Louboutin SAS v. Nakul Bajaj' (2018), the Delhi High Court has required certain e-commerce websites to engage in prior examination of sale listings.
- In Re: Prajwala (2015), the Supreme Court has endorsed the requirement for intermediaries to carry out keyword searches, to flag pedophilic and rape related content, and post warnings to searchers. That said, the committee constituted by the Court to look into the issue of rape and child pornography online highlighted that a solution may lie in *"proactively identifying rogue sites by an independent agency which can identify sites that contains child pornographic and rape-gang rape content and blocking these sites"*. Such a solution would appear to be more in consonance with the Shreya Singhal case, as intermediaries would merely be required to follow the directions of the "independant agency".

124 Notably, this "doctrine" was also later recognised and distinguished by the Delhi High Court in 'Kent RO Ltd. v. Amit Kotak' (2017) from its own judgment pertaining to copyright law. Specifically, the judge noted that the justification provided was that this doctrine of "auto block" laid down in Sabu Mathew George v. Union of India (2017) was in the context of the specific domain of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994, and not under the IT Act or its Rules.

It is unclear how these judicial development are to be reconciled with the Supreme Court's understanding of the obligations of intermediaries in the *Shreya Singhal* decision (which also found approval in the copyright context in the *Myspace* and *Amit Kotak cases*). Arguable, one is seeing a departure from the Shreya Singhal position, atleast in certain limited contexts of content that are seen as extremely dangerous, such as child pornography and gang rape related content.

On the other hand, one has also seen such measures applied in the context of eggregious violations of intellectual property law - which is arguably not as "serious" an issue - thereby possibly pointing to a 'slippery slope' where more and more offences require such pro-active interventions.[125]

In this context, it also becomes important for more streamlined notice requirements to be laid down, with greater coordination between state agencies and relevant intermediaries. One possible method being examined by regulators is to use non-governmental organisations and volunteers to surf the Internet looking for objectionable content, which can then be reported to the intermediaries (who will be required to disable access thereto) (Express News Service, 2018). While prima facie an interesting suggestion, ensuring that these groups are appropriately staffed, trained, transparent, accountable, and neutral, will be a challenge.

5.4. The challenges in asking platforms to "do more"

As discussed in Section 4, courts and regulators have contemplated or are contemplating several new obligations to require intermediaries to "do more" to address a wide variety of online harms. Our analysis in the previous sections also noted that certain common obligations are emerging across contexts and across a variety of online harms. Table 3 below broadly sets out the the types of obligations being imposed on intermediaries and the corresponding harm it seeks to address:

125 For instance, the draft National E-Commerce Policy of 2018, recommends that marketplaces seek authorisation from trademark owners before listing high value goods (irrespective of who uploads such content). Platforms would be required to scan all uploaded content, and then inform a trademark owner in case of any possible infringements. Such a position would appear to conflict with existing case law on the need for automated or generic screening of content by intermediaries.

Table 3 Emerging regulatory obligations for intermediaries in India

Sr no.	Obligations	Harms
1.	Dedicated nodal points for law-enforcement agencies[125]	Hateful rumours,[126] content promoting self-harm,[127] Obscene content[128]
2.	Facilitating pro-active monitoring by law enforcement agencies	Hateful rumours
3.	Identify users upon request from law enforcement agencies or courts	Hateful rumours,[129] defamatory material[130]
4.	"Expeditiously" taking down content brought to their notice.	Hateful rumours
5.	Block access to content on a global basis	Defamatory material
6.	Establish dedicated channels for notices from dedicated agencies and bodies[131]	Hateful rumours, paid political advertisements, sex determination kits,[132] copyrighted and trademarked material
7.	Establish dedicated reporting mechanisms for specific classes of affected users	Obscene content, defamatory, copyrighted and trademarked material
8.	Pro-actively taking down duplicating instances of illegal content previously notified	Sex-determination kits, obscene content, defamatory, copyrighted and trademarked material, counterfeit products[133]
9.	Pre-screening uploaded content	Paid political advertisements,[134] trademarked and copyrighted material, counterfeit products
10.	Develop automated tools to scan for objectionable content	Hateful and obscene content,[135] sexdetermination kits[136]
11.	Establish content moderation policies with trained teams	Hateful and obscene content,[137] sexdetermination kits
12.	Establish an office in India	Hateful rumours, e-commerce platforms
13.	Offer parental controls	Obscene content[138]

We note that several of these are *substantive* obligations that intermediaries, are being required to abide by (despite the absence of any specific statutory mandate). In determining how to impose these obligations, the continuing challenge for both courts and regulators is to determine the appropriate means to do so, particularly in the absence of any legislative intervention on the issue.

We found that, courts tend to impose new obligations in two ways:

- *Within the ambit of Section 79*: We find that, because Section 79 requires intermediaries to observe "due diligence" and adhere to "other guidelines",

the section is effectively being contemplated as an easy route to impose responsibilities on platforms, to ensure users adhere to a wide range of civil and criminal law. There have been efforts by the judiciary to give a wide-reading to the term "due diligence" to impose several substantive obligations on intermediaries.[140] Our analysis indicates that that the term "due diligence" is being used to mitigate against two types of issues: (1) where intermediaries are seen as directly participating in or enabling the commission of an offence; and (2) where they do not adhere to their own terms and conditions and internal policies. [141]

- *Within their contempt of court powers*: Alternatively, there are some cases where courts have imposed 'ad-hoc' obligations through judicial order and have then used their powers of contempt to enforce compliance therewith. For instance, in a recent Madras High Court order, the court clearly stated the reply filed by TikTok outlining the various content moderation and safety features deployed by the platform to tackle the menace of online harms amounted to an undertaking by platform that negative and inappropriate or obscene materials would be filtered and if any violation is found later, the Court would consider it as contempt.[142]

While the use of ad-hoc solutions can be problematic, the basic problem remains that Section 79 is increasingly being used to introduce substantive obligations on intermediaries in a wide variety of contexts.

The statute does not define the terms "due diligence" and "other guidelines" making their scope and ambit unclear. Judicial precedents on Section 79 have not provided any definitive clarification in this regard. An attempt was made by the Andhra Pradesh High Court in Google India Private Limited v. Visaka Industries Limited (2016), where the court noted that the provision requires intermediaries to act with a *"measure of*

140 Refer for instance, to 'Amway India Enterprises Pvt. Ltd. v. 1MG Technologies Pvt. Ltd.' (2019), where the Delhi High Court essentially imposed requirements on the platform to ensure that it does not act so as to procure or induce breach of contracts signed by users/sellers with third parties.

141 See for example 'Amway India Enterprises Pvt. Ltd. v. 1MG Technologies Pvt. Ltd.' (2019).

142 Order dated 24.4.2019 in S. Muthukumar v. The Telecom Regulatory Authority of India (2019)

prudence, activity or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the particular circumstances; not measured by any absolute standard, but depending on the relative facts of the special case."[143] This does not clarify how the obligation to observe "due diligence" would play out in practice or indeed the scope of obligations that can be imposed under Section 79(2)(c). Given that a plain reading of the provision indicates that the provision intends the intermediaries to take due care and attention in carrying out their obligations under the statute, the introduction of completely new obligations (not contemplated anywhere in the IT Act) is questionable. For instance, can this provision be used to require e-commerce platforms to ensure they provide refunds to consumers? Or can it be used to impose de novo taxation obligations on intermediaries? The answers to these questions would appear to be in the negative, given that these substantive obligations are not contemplated in either Section 79 or indeed the rest of the IT Act.

5.5. The need for an evidence-based, consultative and transparent regulatory approach

During our analysis, we noted that, more often than not, it is the judiciary that has been approached first to find ways to deal with and mitigate online harms.[144] The types of directions issued by courts can vary widely - they could range from issuing appropriate blocking orders and other directions to intermediaries,[145] to directing the constitution of expert committees to tackle particularly eggregious online harms[146] to directing the

143 Notably, the court reiterated that *the word "diligence" means careful and persistent application or effort'* and "due diligence" means *"such watchful caution and foresight as the circumstances of the particular case demands."*. The court also quoted the definition of "due diligence" from Words and Phrases by Drain-Dyspnea (Permanent Edition 13A) which defines the word as 'doing everything reasonable, not everything possible'.

144 Petitions are frequently filed before courts claiming the rise of incidence of a specific online harm, with an attendant prayer requesting that the court address a perceived vacuum in regulatory norms. Courts have also permitted affected individuals and entities to directly approach intermediaries in case of violation of certain rights - such as those under intellectual property laws.

145 These directions, as discussed above, can lead to new obligations being immediately imposed on intermediaries, often to ensure "user safety" and to ensure cooperation with law enforcement agencies

146 See, for instance, the constitution of the Ajay Kumar Committee in In Re: Prajwala (2015) to deal with issues concerning online child pornography.

government to come out with a new policies and processes to deal with specific online harms.[147] In some cases, courts go as far as banning entire services. [148]

The proactive stance of Indian courts in relation to a variety of social issues has indeed been essential to protect online users. However, this raises issues pertaining to the broader trend of unelected judges increasingly venturing into policy making (Baxi, 1985). Recent scholarship has shed light upon the problems of policy-making and procedural innovation by judges (Bhuwania, 2015).

The adversarial nature of litigation, while critical in ascertaining fault in specific scenarios, may not be appropriate to discovering ideal policies that can effectively apply to all parties across situations (Bhuwania, 2015).[149] These general concerns are exacerbated in the context of online harms, which require an appreciation of complex technical issues and of the unique nature of online ecosystems.

That said, government-led processes have also been far from satisfactory in terms of the processes followed. Often, when the government is seized of a specific issue, hearings are conducted with internet intermediaries behind closed-doors. In addition, broad commitments may be made on the floor of the Parliament to ensure that internet intermediaries are held more "responsible and accountable" for their services. These tend to be followed with the constitution of internal committees staffed with government officials (with no clear indication of how membership was being decided or how issues and deliberations for such committees are being framed and conducted). The culmination of this cycle is usually a report or a draft policy or regulatory framework, the contents of which are often not made public.

147 For instance, by recommending the establishment of independant agencies to scrutinise the Internet for illegal content in the Sabu Matthew George case.

148 One may consider the banning of TikTok till such time the platform could demonstrate the deployment of various safety measures including pro-active content moderation (S. Muthukumar v. The Telecom Regulatory Authority of India, 2019). Also note that a recent petition before the Kerala High Court has sought a ban on the messaging app Telegram (Tiwari, 2019).

149 Courts are generally concerned with balancing rights inter se the parties before it. More generic policy interventions may however require consideration of effects on stakeholders beyond those appearing in court.

There also appears to be little attention paid to formulating an appropriate evidence base before implementing new policy measures. Often, there is an unclear assessment of the objective of the regulatory intervention, while measures are rarely supplemented with a cost-benefit analyses or regulatory impact assessment. The lack of transparency in these processes makes it difficult to analyse the kinds of problems and solutions being considered. Further, we have also noted scenarios (for instance in the context of the E-Commerce Policy) where measures and obligations are borrowed from the minutae of case-specific court orders, without adequately considering whether such measures are suitable to apply to broader classes of intermediaries.

The problems with such policy making processes can be highlighted by examining two issues that appear to have caught regulatory attention:

- *Criminalisation as an answer to online speech related harms:* The large number of online speech related harms has lead to increased calls for criminalisation of such behaviour. However, opting for crafting new criminal offences may not always be necessary or appropriate to deal with the variety of online harms. It is important to remember that India's statutory framework proscribes a wide variety of online content and conduct, and also gives the state a variety of regulatory tools to deal with online harms.[150]

In such a scenario, rather than opting for crafting new offences as a first step, it may be preferable to:

— Examine existing offences with a view to (a) examining the need to extend the same to the online environment, (b) checking where clarifications are required in view of new forms of commission of offences, as enabled by the Internet.

150 An example of this can be seen in the context of the Supreme Court's decision in Tehseen S Poonawalla v. Union of India (2018), where the court advocated the introduction of new laws to deal with cases of lynching resulting from spread of fake news and rumours. This, despite the IPC already containing several provisions that could be used to address such criminal conduct. Lynching instances can be proceeded against under various provisions of the IPC such as sections pertaining to the use of criminal force, homicide, murder, rioting, rumour mongering etc. While some have argued that mob lynchings are an inherently different offence from that of murder(A. Kumar, 2018), and the signalling effect of special laws also cannot be denied, the need for crafting new (criminal) offences is still unclear in many contexts.

— Examine the reasons behind commission/rise of certain offences, rather than seeking to merely address the medium of communication as a short-term fix or as a silver bullet solution. Technological solutionism cannot be the sole answer to deal with the whole range of online conduct and content related offences (not least as this could lead to progressively more disproportionate fetters on civil liberties). There must be a more thorough examination of risks, and the kinds of action that may be required to mitigate the same, without excessively affecting the nature of the Internet as a cross-border medium of relatively free information exchange.[151]

— Consider the use of measures, short of criminalisation. It is important to remember that merely creating new criminal laws in and of itself would be insufficient to deal with online harms, particularly in view of the enforcement problems in the online context. This may include, for instance, conducting awareness and education campaigns amongst both the public and amongst law enforcement officials on the scope of existing laws, and the existing methods that can be used to tackle online harms. This aspect has also been noted by courts in a number of cases, for instance, when recommending the adoption of better coordination mechanisms between intermediaries and courts, tie-ups with civil society organisations, and creation of independent agencies to scrutinise online content.

- *Requiring localisation of user data:* In view of a perceived inability to enforce Indian law online, there have been calls (from the government and the judiciary) to impose "data localisation" norms. However, the reasons for this are usually unarticulated (or not captured adequately by court orders) and in the circumstances, it is unclear if putting in place such requirements will be a proportionate response to a problem that is as yet unclear, and could possibly be ameliorated through alternative, less intrusive means.(Bailey & Parsheera, 2018).

151 This may involve the creation of different regulatory frameworks pertaining to different types of harms, as has been done for instance, in the context of intellectual property violations.

Rather than try and ensure Indian law applies to each and every instance of cross-border harm, which may be impractical and lead to disproportionate censorship, it may be preferable for (a) the state to take network level measures to limit access to certain types of content or certain services, only in the event of severe or persistent violations of Indian law that lead to a relatively substantial risk to users in India or only in cases of extremely severe harms (for instance child pornography, etc.), (b) look to forge global consensus on how to deal with cross-border harms and to promote cooperation between law enforcement agencies in different countries. Finally, there is also an education and capacity building element that must be given adequate consideration.

6. Conclusion

In recent years, rising Internet access has brought with it concerns regarding various online harms that take place through the services of various intermediaries. States are increasingly looking at methods and mechanisms to make the digital ecosystem safer, including by re-evaluating the responsibilities cast on intermediaries in this respect. A core public policy issue in this respect has concerned the balancing of "safe harbour" afforded to intermediaries (for carrying third party content), with the imposition of greater obligations.

In this paper, we sought to examine the evolving regulatory framework around online harms and specifically the responsibilities sought to be placed on intermediaries to ameliorate such harms. We focused on seven broad categories of "online harms" that have been sites for regulatory interventions. We also identified certain new and emerging harms that are increasingly capturing public and regulatory attention.

We demonstrate that much regulatory attention has been on specific categories of internet intermediaries, most notably social media platforms, e-commerce platforms, and search engines. However, the current statutory framework under the IT Act lacks clarity on whether obligations can be imposed on specific types of intermediaries. There

may therefore be a need to re-examine this statutory framework to ensure that the statute permits the imposition of narrowly tailored obligations, rather than adopting a "one-size-fits-all" approach.

We found that, in some cases, some obligations (particularly those to generally monitor content on an *ex-ante* basis) can run contrary to existing jurisprudence on what intermediaries can and cannot be expected to do. Further, clarifications may also be required regarding the nature and scope of self-regulatory efforts that are being increasingly expected from intermediaries, especially to ensure that such efforts do not unduly impact the rights and interests of users.

In addition, the routes adopted to impose such obligations - through an exercise of contempt of court powers or through the framework of Section 79 - are ad-hoc responses, creating a patchwork of obligations on intermediaries, that may not necessarily be consistent or proportionate. Our analysis indicates that,in light of the approaches being adopted by courts, there may be a need to re-examine the statutory framework of Section 79 itself, to appropriately define the expected "due diligence" from different types of intermediaries.

Finally, we underscore that the judiciary has been the primary agent of evolving tools and mechanisms to address issues of user safety in the online space. There are clear signs of an activist approach, with courts engaging in judicial policymaking in many scenarios, such as when tackling obscene content, defamatory conduct or hateful or abusive online activity. The focus for courts has been on increasing obligations on intermediaries by requiring them to either monitor online activity, filter online content, and otherwise work with regulators and law enforcement agencies to ensure that Indian laws can be properly enforced in the digital ecosystem. While the intent to address online harms is indeed understandable, the increasing regulation of the Internet through judicial efforts has also meant that the process of making policy choices for the Internet is inadequately democratic. Judicial processes are not designed to consider the panopoly of interests and issues that may arise in the context of online regulation - they are by nature designed to balance rights *inter se* specific parties.

However, government interventions too have been largely sporadic and fragmented, and are often knee-jerk reactions to public outcry (or indeed only taken up when directed to do so by courts). Such a reactionary approach may not always strike a succesful balance between the various interests that are required to be considered in the context of online regulation - such as civil liberties, economic interests and state interests concerning the enforcement of laws. This points to the need for a rigorous, sufficiently transparent and participatory process of policy-making - one that can clearly specify the harms sought to be addressed, and contemplate targeted obligations keeping in mind the unique characteristics of online ecosystems and the different types of intermediaries.

7. Annexure: The Current Regulatory Framework

Indian law currently uses both the IT Act and certain sector-specific regulations to classify and place various obligations on different types of intermediaries. These are briefly discussed below:

7.1. Existing obligations on intermediaries

The IT Act contains a number of obligations that all intermediaries are required to adhere to. These are primarily designed to reduce harm to users and networks, and to ensure compliance with government/court directions particularly in relation to blocking of content and enabling the investigation of offences. Some of the more important obligations cast on intermediaries include:

- The need for intermediaries to retain data as mandated by the Central Government;[152]

152 Section 67C of the IT Act empowers the Central Government to mandate the retention of any categories of information by any intermediary. The government can also specify the duration and format of data retention. As on date, the Government has only laid down norms pertaining to a specific category of intermediaries - those engaged in providing 'digital locker facilities'. See Information Technology (Preservation and Retention of Information by Intermediaries providing Digital Locker Facilities) Rules, 2016.

- To "extend all facilities and technical assistance" to facilitate the interception, monitoring or decryption of any information stored on a computer resource;[153]
- To ensure necessary cooperation and reporting pertaining to cyber security incidents and to maintain privacy and security of user data;[154]
- To block access to online content under Section 69A of the IT Act. [155]

Some intermediaries are regulated under sectoral frameworks. For instance, internet service providers are bound by the terms of the licenses granted to them by the government as well as regulations framed by the Telecom Regulatory Authority of India (TRAI). Similarly, cab aggregator are subject to the rules adopted by State Governments to govern the conduct of on-demand transport aggregators, and providers of digital payment services are governed by the rules formulated by the Reserve Bank of India (RBI).

7.1.1. "Safe harbour" under the IT Act

The framework dealing with the liability of intermediaries for storing / transmitting / hosting third-party content is set out under two statutes: (a) the IT Act (and the Information Technology (Intermediary Guidelines) Rules, 2011); and (b) the Copyright Act, 1957 (and the Copyright Rules of 2013).

Section 79(1) of the IT Act, provides that intermediaries are not to be held liable for any third party information on their platforms. However,

- The exemption from liability is applicable only if the intermediary - (a) provides temporary storage or transmission functions, or (b) does not initiate/select

153 See Section 69 of the IT Act. Note that the constitutionality of this provision is currently under challenge before the Supreme Court on the grounds of violating the right to privacy (Bailey, Bhandari, Parsheera & Rahman, 2018). Also see the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

154 Section 43A and Section 72A of the IT Act. Further, certain categories of intermediaries are also required to maintain privacy of user data under sector specific laws, regulations and contracts - for instance, telecom service providers under the terms of their licenses, and payment systems under regulations framed by the Reserve Bank of India.

155 This section empowers the Central Government to direct an intermediary to block public access to "any information generated, transmitted, received, stored or hosted in any computer resource". Failure to comply with a direction is punishable with imprisonment of upto seven years and a fine. The procedures and safeguards for the issuance of blocking directions are contained in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

the receiver of the transmission or select or modify the information in the transmission. Essentially, the provision requires intermediaries to act more or less as "dumb pipes" - to not knowingly, intentionally and actively aid and enable the commission of an offence - in order to claim the benefit of the exemption.

- Intermediaries must remove or disable access to unlawful content (without vitiating any evidence) in an expeditious manner upon receiving 'actual knowledge' thereof. The Supreme Court has 'read-down' the provision in (v. Union of India, 2016) to clarify that an intermediary can only gain "actual knowledge" of an offence when informed through lawful procedures specified under the IT Act i.e. when informed by the competent government agencies or a court.[156]

- Intermediaries must exercise "due diligence" in the exercise of their duties under the IT Act and other guidelines specified by the Central Government. The Information Technology (Intermediaries Guidelines) Rules, 2011, provide for the nature of due diligence to be observed by intermediaries. Under these rules, intermediaries must *inter alia*:

    — Publish terms of service and a privacy policy for usage of its service by any user;

    — Ensure that users are warned against uploading various categories of proscribed content;

    — Inform users that they could lose access to their services if they breach any rules or regulations, terms of service or privacy policy;[157]

    — Take reasonable measures to secure its computer resource;

156 The Supreme Court specifically recognised the difficult situation intermediaries could face if required to judge the legitimacy or otherwise of millions of requests for blocking content.

157 The rules also contain requirements for intermediaries to take-down unlawful content or disable access to any information, on obtaining actual knowledge of such content either by itself or on the receipt of private complaints. Take-downs based on private complaints were to be carried out within one month of the complaint being made. These parts of the rule were rendered null by the Shreya Singhal decision.

— Provide information to lawfully authorised government agencies, when required to do so by a lawful order;[158]

— Follow the provisions of the IT Act and rules thereunder;

— Report cyber security incidents to relevant government agencies.

7.1.2. "Safe harbour" under the Copyright Act

Similar to the IT Act, the Copyright Act, 1957 also contains a safe harbour provision protecting intermediaries from liability for copyright infringement by third parties. While the provision does not refer specifically to 'intermediaries', it applies to any person who offers "transient or incidental storage" of a work or performance for providing electronic access to it.

However, unlike the IT Act, which requires intermediaries to take-down content only pursuant to a Government or court order, the copyright law allows the owner of copyright to also initiate a takedown request (i.e. the intermediary must comply with a take-down process in order to claim the benefit of the "safe harbour").

Intermediaries who receive a written complaint of an infringement from a copyright owner must block access to the allegedly infringing content for a period of 21 days. During this period the copyright owner must produce a court order to formalise the restriction, failing which the content can be restored.

158 Intermediaries must provide "information or any such assistance" to lawfully authorised government agencies to enable the verification of user identities, and to prevent/detect/investigate/prosecute cyber security and other offences.

References

Abraham, B. (2018). More than 2000 people watched a man live streaming his suicide on facebook, and nobody bothered to alert police. Retrieved from https://tinyurl.com/rq8hnwh

Adeane, A. (2019). Blue whale: What is the truth behind an online 'suicide challenge'? Retrieved from https://www.bbc.com/news/blogs-trending-46505722

Agarwal, S. (2017). Information technology ministry asks google, facebook, whatsapp and instagram to remove blue whale game links. Retrieved from https://economictimes.indiatimes.com/magazines/panache/it-ministry-asks-google-facebook-whatsapp-and-instagram-to-remove-blue-whale-game-links/articleshow/60070772.cms?from=mdr

Agarwal, S. C. (2018). More pressure on whatsapp! government says trace origin of messages to fight fake news. Retrieved from https://www.businesstoday.in/current/economy-politics/it-ministry-to-dash-off-third-letter-to-whatsapp-reiterating-demand-for-message-traceability/story/282626.html

Aggarwal, S. (2018a). Govt asks whatsapp to immediately stop spread of "irresponsible" and "explosive" messages. Retrieved from https://bit.ly/31irplU

Aggarwal, S. (2018b). Peeved with whatsapp's reply, india prepares to tighten leash on internet firms. Retrieved from https://economictimes.indiatimes.com/tech/internet/to-stop-rumour-mill-government-readies-rules-for-net-companies/articleshow/65508578.cms?from=mdr

Aiyappa, M. (2018). Karnataka mulls framing law to sell liquor online. Retrieved from https://timesofindia.indiatimes.com/city/bengaluru/karnataka-mulls-framing-law-to-sell-liquor-online/articleshow/66290271.cms

Allcott, H. & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31* (2), 211-236. Retrieved from https://web.stanford.edu/~gentzkow/research/fakenews.pdf

Amway India Enterprises Pvt. Ltd. v. 1MG Technologies Pvt. Ltd. (2019). CS (OS) 410/2018.

Anand, N., Thomas, C., Jain, P., Bhat, A., Thomas, C., Prathyusha, P., ... Cherian, A. (2018). Internet use behaviors, internet addiction and psychological distress among medical college students: A multi centre study from south india. *Asian Journal of Psychiatry, 37.* Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/30145540

Aneez, Z., Neyazi, T. A., Kalogeropoulos, A. & Nielsen, R. K. (2019). *India Digital News Report 2019.* Reuters Institute for the Study of Journalism. Retrieved from https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-03/India_DNR_FINAL.pdf

Anonymous. (2018). India lynchings: Whatsapp sets new rules after mob killings. Retrieved from https://www.bbc.com/news/world-asia-india-44897714

Antony Clement Rubin v. Union of India. (2019). W.P. No. 20774/2018.

Arun, C. (2014). Filtering content on the internet. Retrieved from https://www.thehindu.com/opinion/op-ed/Filtering-content-on-the-internet/article11640692.ece

Arun, C. (2019). On whatsapp, rumours, lynchings and the indian government. *Economic and Political Weekly.* Retrieved from http://tiny.cc/zm479y

Arvinder Singh v. State of Punjab. (2018). CRM-M No. 43622/2017.

Ashwath v. The State. (2017). Criminal Petition No. 200644/2017.

Associated Press. (2019). White house launches site where you can report anticonservative bias from tech giants. Retrieved from https://www1.cbn.com/cbnnews/politics/2019/may/white-house-launches-site-where-you-can-report-anti-conservative-bias-from-tech-giants

Bailey, R., Bhandari, V., Parsheera, S. & Rahman, F. (2018). Use of personal data by intelligence and law enforcement agencies. Retrieved from https://bit.ly/2CEzCoN

Bailey, R. & Parsheera, S. (2018). Data localisation in india: Questioning the means and ends. *NIPFP Working Paper 242.* Retrieved from https://bit.ly/2R8Q8lW

Bailey, R., Parsheera, S. & Rahman, F. (2018). Comments on the (draft) information technology [intermediaries guidelines (amendment) rules], 2018. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328401

Barik, S. (2020). Delhi hc issues notice to meity and twitter on the suspension of sanjay hegde's account. Retrieved from https://www.medianama.com/2020/01/223-delhi-hc-sanjay-hegde-notice-to-twitter-meity/

Baruah, J. (2017). Blue whale challenge and other 'games' of death. Retrieved from https://m.economictimes.com/magazines/panache/blue-whale-challenge-and-other-games-of-death/articleshow/60135835.cms

Baxi, U. (1985). Taking suffering seriously: Social action litigation in the supreme court of india. *Third World Legal Studies.* Retrieved from https://bit.ly/ 2RaBhLN

Bhargava, M. (2018). Suicide and technology: Partners in crime? Retrieved from https://www.thehindubusinessline.com/specials/technophile/using-technology-and-ai-to-prevent-suicides/article24936734.ece

Bhatnagar, G. V. (2017). Sc closes katju contempt case, but questions about individual liberty persist. Retrieved from https://thewire.in/rights/sc-closes-katju-contempt-case-questions-individual-liberty-persist

Bhuwania, A. (2015). *Media freedom as a fundamental right.* Cambridge University Press.

Bijumon v. The State of Kerala. (2018). 2018 (4) KHC 73.

Board, E. (2019). When the law becomes a weapon of intimidation. Retrieved from https://www.telegraphindia.com/opinion/contempt-of-court-case-against-patricia-mukhim-when-the-law-becomes-a-weapon-of-intimidation/cid/1687021

Bureau, B. I. T. (2019). 'difficult to ban pubg': Indian government leaves it up to the parents. Retrieved from https://www.businessinsider.in/difficult-to-ban-pubg-indian-government-leaves-it-up-to-the-parents/articleshow/70603348.cms

Caplan, R., Hanson, L. & Donovan, J. (2018). Dead reckoning. Retrieved from https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf

Centre for Democracy and Technology. (2012). Shielding the messengers protecting platforms for expression and innovation. Retrieved from https://cdt.org/wp-content/uploads/pdfs/CDT-Intermediary-Liability-2012.pdf

Centre for the Study of Developing Societies. (2019). Social media and political behaviour. Retrieved from https://www.csds.in/uploads/custom_files/Report-SMPB.pdf

Chan, M. (2018). Kids are playing the 'choking game' to get high. instead, they're dying. Retrieved from https://time.com/5189584/choking-game-pass-out-challenge/

Children's Online Privacy Protection Rule. (2013). Retrieved from https://bit.ly/2SnntyB

Chisti, S. (2018). Prescription post section 66a: 'change law to punish hate speech online'. Retrieved from https://indianexpress.com/article/india/hate-speech-online-punishment-supreme-court-section-66a-information-technology-act-narendra-modi-4876648/

Christian Louboutin SAS v. Nakul Bajaj. (2018). Civil Suit No. 344/2018.

Christopher, N. (2018). Pepsi sues facebook, twitter, hc orders posts to be taken down that allege kurkure contains plastic. Retrieved from http://tiny.cc/pf85iz

Consim Info Pvt. Ltd. v. Google India Pvt. Ltd. (2013). 2013 (54) PTC 578 (Mad).

Court in its own motion v. S Gurumurthy. (2018). Cont. Cas (Cr) 17/2018.

Dahat, P. (2018). Scribe charged with sedition over fb post. Retrieved from https://www.thehindu.com/news/national/other-states/scribe-charged-with-sedition-over-fb-post/article23731882.ece

Das, S. & Gupta, K. (2018). Centre tells states to keep tabs on rumours, prevent lynchings. Retrieved from https://bit.ly/2SeIedB

Deep, A. (2018a). Pepsico gets john doe order to take down thousands of tweets and posts on kurkure, even jokes. Retrieved from https://www.medianama.com/2018/07/223-pepsico-kurkure-twitter-facebook-order/

Deep, A. (2018b). Why should we talk to dunzo? state regulators fume at liquor delivery. Retrieved from https://www.medianama.com/2018/09/223-why-should-we-talk-to-dunzo-state-regulators-fume-at-liquor-delivery/

Deloitte and Indian Music Industry. (2019). *Economic impact of the recorded music industry in india.* Retrieved from https://bit.ly/36bwAq1

Desk, T. (2019). Pubg caused the death of mp teen, here are 5 other online games that have proved fatal. Retrieved from https://www.news18.com/news/buzz/pubg-caused-the-death-of-mp-teen-here-are-5-other-online-games-that-have-proved-fatal-2166867.html

Directive of the European Parliament and of the Council on electronic commerce. (2000). 2000/31/EC).

Doshi, V. (2016). Facebook under fire for 'censoring' kashmir-related posts and accounts. Retrieved from https://www.theguardian.com/technology/2016/jul/19/facebook-under-fire-censoring-kashmir-posts-accounts

Dutta, A. N. (2018). Panel formed by modi's office to fix india's internet, from fake news to payments. Retrieved from https://theprint.in/india/governance/india-has-no-way-to-tackle-fake-news-or-cyber-crime-this-panel-aims-to-change-that/117272/

Dutta, P. K. (2018). 16 lynchings in 2 months. is social media the new serial killer? Retrieved from https://www.indiatoday.in/india/story/16-lynchings-in-2-months-is-social-media-the-new-serial-killer-1275182-2018-07-02

Egelhofer, J. L. & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: A framework and research agenda. *Annals of the International Communication Association.* Retrieved from https://www.tandfonline.com/doi/full/10.1080/23808985.2019.1602782

Election Commission of India. (2019a). Reconstitution of media certification and monitoring committee. Retrieved from https://bit.ly/2vPdjwV

Election Commission of India. (2019b). Report of the committee on section 126 of the representation of the people act, 1951. Retrieved from https://eci.gov.in/files/file/9276-report-of-the-committee-on-section-126-of-the-representation-of-the-people-act-1951/

Electronic Frontier Foundation. (2019). Eff project shows how people are unfairly "tossed out" by platforms' absurd enforcement of content rules. Retrieved from https://www.eff.org/press/releases/eff-project-shows-how-people-are-unfairly-tossed-out-platforms-absurd-enforcement

Express News Service. (2018). Law against lynching: Committee submits report to gom. Retrieved from https://indianexpress.com/article/india/law-against-lynching-committee-submits-report-to-gom-5331814/

Fazili, S. (2018). Whatsapp messages and the mad mob lynching: A timeline. Retrieved from https://www.news18.com/news/india/whatsapp-messages-and-the-mad-mob-lynching-a-timeline-1798135.html

Federal Government of Germany. (2017). The Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG). Retrieved from https://germanlawarchive.iuscomp.org/?p=1245

Film Society v. Union of India. (2018). 2018 (6) Bom CR 270.

Frosio, G. (2016). From horizontal to vertical: An intermediary liability earthquake in europe. *Journal of Intellectual Property Law and Practice, 12.* Retrieved from https://bit.ly/2vuCiFF

Ganjoo, S. (2019). First case of netflix addiction documented in india. Retrieved from https://www.indiatoday.in/technology/news/story/first-case-of-netflix-addiction-documented-in-india-1359343-2018-10-09

Gayatri v. State. (2017). W.P.(CRL) 3083/2016.

Ghosh, S. (2015). Porn websites ban: Govt puts the onus on isps. Retrieved from https://www.livemint.com/Politics/7UydgLiaahBL13UnmOG6BK/Ban-on-websites-without-child-pornography-lifted.html

Gillespie, T. (2018). Platforms are not intermediaries. *Georgetown Law Technology Review.* Retrieved from https://georgetownlawtechreview.org/platforms-are-not-intermediaries/GLTR-07-2018/

Goel, I. (2018). Why more and more people are committing suicide before a live online audience. Retrieved from https://indianexpress.com/article/lifestyle/health/committing-suicide-online-live-streaming-facebook-5309827/

Google India Private Limited v. Visaka Industries Limited. (2016). 2017(1)ALT620.

Government of Australia. (2019). Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill, 2019. Retrieved from http://tiny.cc/2xeqgz

Government of India. (2017). Measures to Curb Online Child Sexual Abuse Material (CSAM).

Government of the United States of America. (1998). Children's Online Privacy Protection Act.

Government of the United States of America. (2018). Allow States and Victims to Fight Online Sex Trafficking Act.

Greenberg, P. (2018). Children and the internet: Laws relating to filtering, blocking, and usage policies in schools and libraries. Retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/state-internet-filtering-laws.aspx

Grover, D. (2019). India has world's second-largest internet user base. Retrieved from https://www.bloombergquint.com/technology/india-has-worlds-second-largest-internet-user-base

Hopf, H., Krief, A., Mehta, G. & Matlin, S. A. (2019). Fake science and the knowledge crisis: Ignorance can be fatal. *Royal Society Open Science, 6*(5), 190161. Retrieved from https://royalsocietypublishing.org/doi/abs/10.1098/rsos.190161

HT Correspondent. (2016a). Police have court orders to block 316 obscene sites, govt tells hc. Retrieved from https://www.hindustantimes.com/mumbai/police-have-court-orders-to-block-316-obscene-sites-govt-tells-hc/story-Ol0FBdSbHmjPxDxkIdL7cO.html

HT Correspondent. (2016b). When online liquor sale 'start-up' delivered to cops, and got arrested. Retrieved from https://www.hindustantimes.com/punjab/how-to-sell-liquor-online-and-get-arrested-get-talli-lesson-chandigarh/story-LYRz9tEfbSnmw2VIj2D0VJ.html

IANS. (2016). Bengal: 17-years-old girl commits suicide due to obscene social media posts. Retrieved from https://tinyurl.com/tmrxfvq

IANS. (2018a). Trolled on social media, nri girl in uae planned to livestream suicide, saved in nick of time. Retrieved from https://tinyurl.com/sre2gp6

IANS. (2018b). Whatsapp to restrict india service as government talks tough. Retrieved from https://www.moneylife.in/article/whatsapp-to-restrict-india-service-as-government-talks-tough/54766.html

IANS. (2019). Should social media live-streaming be banned? Retrieved from https://economictimes.indiatimes.com/tech/internet/should-social-media-live-streaming-be-banned/articleshow/68546583.cms?from=mdr

In Re: In the matter of incidence of gangrape in a boarding school situated in Bhauwala, District Dehradun v. State of Uttarakhand. (2018). WP (PIL) 158/2018.

In Re: Prajwala. (2015). SMW Crl. No. 3/2015.

Internet and Mobile Association of India. (2019). Voluntary code of ethics for the 2019 general election. Retrieved from https://eci.gov.in/files/file/9467-social-media-platforms-present-voluntary-code-of-ethics-for-the-2019-general-election-to-election-commission-of-india/

Internet Freedom Foundation. (2019). Why is porn being blocked in india? Retrieved from https://internetfreedom.in/why-is-porn-being-blocked-in-india-whattheblock/

Jalan, T. (2019a). Centre will change terms of uidai's proposed social media monitoring agency: Agi. Retrieved from https://www.medianama.com/2018/09/223-agi-sc-uidai-social-media-monitoring-agency/

Jalan, T. (2019b). Delhi hc hears out petition demanding ban on online gambling websites; 'what makes you special?', chief justice asks aigf. Retrieved from https://www.medianama.com/2019/08/223-what-makes-you-special-chief-justice-of-delhi-hc-asks-aigf-in-petition-demanding-ban-on-online-gambling-websites/

Janani Krishnamurthy v. Union of India. (2019). W.P. No. 20214/2018.

Jha, F. & Taskin, B. (2019). Blue tick not just a verification but a mark of twitter's caste bias, say users. Retrieved from https://theprint.in/india/blue-tick-not-just-a-verification-mark-but-a-mark-of-twitters-caste-bias-say-users/316475/

Jha, L. (2019). How the govt is cracking down on film piracy. Retrieved from https://www.livemint.com/industry/media/how-the-govt-is-cracking-down-on-film-piracy-1550130158629.html

Kamlesh Vaswani v. The Union of India. (2018). 2019 (1) CTC 548.

Keller, D. (2018). Internet platforms: Observations on speech, danger, and money. *Hoover Institution Essay, Aegis S Paper No. 1807.* Retrieved from https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money

Kent RO Ltd. v. Amit Kotak. (2017). 2017 (69) PTC 551 (Del).

Khattar, A., Dabas, K., Gupta, K., Chopra, S. & Kumaraguru, P. (2018). White or blue, the whale gets its vengeance: A social media analysis of the blue whale challenge. Retrieved from http://precog.iiitd.edu.in/pubs/white-blue-whale.pdf

Kishorchandra Wangkhem v. The District Magistrate, Imphal West Government of Manipur. (2019). Writ Petition (Cril) No. 18/2018.

Koops, B.-J. (2010). The internet and its opportunities for cybercrime. *Transnational Criminology Manual.* Retrieved from https://pure.uvt.nl/portal/en/publications/the-internet-and-its-opportunities-for-cybercrime(cacedf83-6d90-404d-b4f8-fa92081234cc).html

Kovacs, A. & Nayantara, R. (2017). Criminal law and freedom of expression on the internet in india. Retrieved from https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf

Kumar, A. (2018). Lynchings aren't just murders. we need specific data on it – and now. Retrieved from https://www.thequint.com/voices/opinion/absence-of-data-on-lynching-modi-government

Kumar, S. & India Today Web Desk. (2019). Upset over failed love, alwar man live streams suicide on facebook for around 2 hours. Retrieved from http://tiny.cc/cvso9y

Law Commission of India. (2017). *267th report of the law commission of india on hate speech.* Retrieved from http://lawcommissionofindia.nic.in/reports/Report267.pdf

Lazar, D., Baum, M., Benkler, Y., Berinsky, A., Greehill, K., Menczer, F., ... Zittrain, J. (2018). The science of fake news. *Science, 359*(6380), 1094–1096. Retrieved from https://science.sciencemag.org/content/359/6380/1094.full.pdf

Li, T. (2018). Intermediaries and private speech regulation: A transatlantic dialogue. Retrieved from https://law.yale.edu/sites/default/files/area/center/isp/documents/private_speech_reg_workshop_report_3.12.19.pdf

Luxottica Group S.P.A. v. Mify Solutions Pvt. Ltd. (2018). CS (COMM) 453/2016.

Mandavia, M. (2019). India asks whatsapp to fingerprint messages to ensure tracebility. Retrieved from https://tech.economictimes.indiatimes.com/news/mobile/india-asks-whatsapp-to-fingerprint-messages-to-ensure-traceability/69833913

Mandhani, A. (2019). Why baba ramdev's win against facebook, google in delhi hc only adds to judicial confusion. Retrieved from https://theprint.in/india/governance/judiciary/why-baba-ramdevs-win-against-facebook-google-in-delhi-hc-only-adds-to-judicial-confusion/312403/

Manglik, R. (2017). Not only blue whale challenge, these 5 insane online games are also dangerous for your kids. Retrieved from https://www.indiatvnews.com/buzz/life-blue-whale-challenge-and-other-insane-online-games-that-cause-teenager-deaths-399056

Mantri, G. (2018). Now, online sale of pets comes under the purview of law. Retrieved from https://www.thenewsminute.com/article/now-online-sale-pets-comes-under-purview-law-88248

McLaughlin, T. (2018). How whatsapp fuels fake news and violence in india. Retrieved from https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/

Mehdi Masroor Biswas v. State of Karnataka. (2018). Criminal Petition No. 8749/2016.

Mehrotra, K. (2018). Private member's bill in lok sabha to propose alternatives to it act draft amendments. Retrieved from https://indianexpress.com/article/india/private-members-bill-in-lok-sabha-to-propose-alternatives-to-it-act-draft-amendments-5512610/

Mehta, I. (2019). After the us, twitter faces wrath from india's right wing over alleged bias. Retrieved from https://thenextweb.com/in/2019/02/12/after-the-us-twitter-faces-wrath-from-indias-right-wing-over-alleged-bias/

Microsoft News Center India. (2019). Civility, safety and interaction online. Retrieved from https://news.microsoft.com/en-in/microsoft-digital-civility-index-safer-internet-day-2019/

Ministry of Electronics and Information Technology. (2017). Advisory on blue whale challenge game. Retrieved from https://www.meity.gov.in/advisory-blue-whale-challenge-game

Ministry of Electronics and IT. (2018). Draft it rules issued for public consultation. Retrieved from https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1557159

Ministry of Foreign Affairs and Trade, Government of New Zealand. (2019). Christchurch call to eliminate terrorist and violent extremist content online. Retrieved from https://www.christchurch-call.com

Mohan, A. M. (2009). India among top 10 in net piracy. Retrieved from https://www.livemint.com/Politics/5LQ64iULAYiNprY2dhFVwI/India-among-top-10-in-net-piracy.html

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy, 3* (1), 39–43. Retrieved from https://doi.org/10.1080/23738871.2018.1462395

Myspace Inc. v. Super Cassettes Industries Ltd. (2017). 236 (2017) DLT 478.

Narayanan, V., Kollanyi, B., Hajela, R., Barthwal, A., Marchal, N. & Howard, P. N. (2019). News and information over facebook and whatsapp during the indian election campaign. Retrieved from https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-memo.pdf

National Crime Records Bureau. (2017). *Crime in India, 2016.* Government of India. Retrieved from http://tiny.cc/gqyj9y

National Intellectual Property Rights Policy. (2016). Retrieved from https://dipp.gov.in/sites/default/files/National_IPR_Policy_English.pdf

Natrajkumar, N. (2019). Man live-streams suicide on facebook; viewers post sad emojis but don't stop lovelorn victim. Retrieved from https://www.ibtimes.co.in/man-live-streams-suicide-facebook-viewers-post-sad-emojis-dont-stop-lovelorn-victim-799824

Ofcom. (2018). *Addressing Harmful Online Content.* Retrieved from https://www.ofcom.org.uk/_data/assets/pdf_file/0022/120991/Addressing-harmful-online-content.pdf

Pahwa, N. (2018). I and b ministry looks to regulate digital broadcast and news; fake news to lead to de-accreditation of journalists. Retrieved from https://www.medianama.com/2018/04/223-media-accredition-smriti-irani/

Parliamentary Standing Committee. (2007). *Report on the information technology (amendment) act, 2006.* Retrieved from https://bit.ly/2DFqv9f

Parmeshwar Bharati v. State of U.P. (2018). 2019 (1) ACR 795.

Pathare, S. (2017). Blue whale is a red herring: Let's talk about suicides, shall we? Retrieved from https://thewire.in/health/blue-whale-challenge-red-herring-suicide-prevention

PepsiCo India Holdings Pvt. Ltd. v. Facebook, Inc. (2018). CS (OS) No. 80/2018.

Perset, K. (2010). *The Economic and Social Role of Internet Intermediaries.* Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/internet/ieconomy/44949023.pdf

Pradhan, D. (2018). Gauba committee recommends 'criminal proceedings' against social media spreading fake news. Retrieved from https://inc42.com/buzz/gauba-committee-recommends-criminal-proceeding-against-social-media-spreading-fake-news/

Prakash, P. (2012). Analysing latest list of blocked sites (communalism and rioting edition). Retrieved from https://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism

Prakash, P. (2016). List of blocked 'escort service' websites. Retrieved from https://cis-india.org/internet-governance/blog/list-of-blocked-escort-service-websites

Prasad, R. S. (2018). Statement in reply to rajya sabha starred question no. 184 for 3.8.2018 regarding spreading fake news in social media. Retrieved from https://www.medianama.com/wp-content/uploads/As184.pdf

Press Trust of India. (2015). Delhi government set to crackdown on online sites selling liquor. Retrieved from https://www.ndtv.com/delhi-news/delhi-government-set-to-crackdown-on-online-sites-selling-liquor-1229419

Press Trust of India. (2016a). Blocking websites with escort services doesn't fix the problem, says deity. Retrieved from https://www.indiatoday.in/technology/news/story/blocking-websites-with-escort-services-doesnt-fix-the-problem-says-deity-14604-2016-06-16

Press Trust of India. (2016b). Pil seeks police action against website ads on escort services. Retrieved from https://www.dnaindia.com/india/report-pil-seeks-police-action-against-website-ads-on-escort-services-2204362

Press Trust of India. (2017). Photograph on social media leads woman to suicide, 3 booked. Retrieved from https://www.mid-day.com/articles/photograph-on-social-media-leads-woman-to-suicide-3-booked/18844173

Press Trust of India. (2018a). At aiims, internet addiction patients have doubled in last 2 years. Retrieved from https://bit.ly/2vIUgnX

Press Trust of India. (2018b). Centre withdrawing notification on social media hub, ag informs supreme court. Retrieved from https://bit.ly/3b20249

Press Trust of India. (2018c). Indecent depiction of women on digital platforms proposed to be made punishable. Retrieved from https://timesofindia.indiatimes.com/india/indecent-depiction-of-women-on-digital-platforms-proposed-to-be-made-punishable/articleshow/64454904.cms

Press Trust of India. (2018d). Law against indecent representation of women on digital platforms in the works. Retrieved from https://thewire.in/women/indecent-depiction-women-digital-platforms-punishable

Press Trust of India. (2018e). Whatsapp to build india team as part of reported steps to curb fake news. Retrieved from https://gadgets.ndtv.com/apps/news/whatsapp-to-build-india-team-as-part-of-reported-steps-to-curb-fake-news-1895773

Press Trust of India. (2019). 155 isis operatives, sympathisers arrested so far in india: Home ministry. Retrieved from https://www.ndtv.com/india-news/155-isis-operatives-sympathisers-arrested-so-far-in-india-home-ministry-2059073

PRS Legislative Research. (2013). The indecent representation of women (prohibition) amendment bill, 2012. Retrieved from https://www.prsindia.org/billtrack/the-indecent-representation-of-women-prohibition-amendment-bill-2012-2576

Reporter, S. (2019). Case registered on eci's plaint on fake news. Retrieved from https://www.thehindu.com/news/cities/Delhi/case-registered-on-ecis-plaint-on-fake-news/article26369275.ece

Reuters. (2019). Whatsapp launches fact-check service to fight fake news during india polls. Retrieved from https://tech.economictimes.indiatimes.com/news/internet/whatsapp-launches-fact-check-service-to-fight-fake-news-during-india-polls/68686216

S. Muthukumar v. The Telecom Regulatory Authority of India. (2019). WP (MD) No. 7855 of 2019.

Sabu Mathew George v. Union of India. (2017). (2017) 2 SCC 514.

Safi, M. (2018). 'whatsapp murders': India struggles to combat crimes linked to messaging service. Retrieved from https://www.theguardian.com/world/2018/jul/03/whatsapp-murders-india-struggles-to-combat-crimes-linked-to-messaging-service

Sanghvi, V. (2018). India's lynching app: Who is using whatsapp as a murder weapon? Retrieved from https://www.scmp.com/week-asia/society/article/2154436/indias-lynching-app-who-using-whatsapp-murder-weapon

Scaria, A. G. (2013). Online piracy of indian movies: Is the film industry firing at the wrong target. *Michigan State International Law Review.* Retrieved from https://bit.ly/2qySCTt

Sebastian, M. (2017). Expert panel suggests amendments to curb online hate speech. Retrieved from https://www.livelaw.in/expert-panel-suggests-amendments-curb-online-hate-speech/

Secretary of State for Digital, Culture, Media and Sport & Secretary of State for the Home Department. (2019). *Online Harms White Paper.* Government of UK. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Shakil, S. (2019). 257 entries of 'fake news' in ncrb records. Retrieved from https://www.newindianexpress.com/nation/2019/oct/22/fake-news-in-ncrb-records-257-entries-2051173.html

Shrivastava, K. (2018). 40 government departments are using a social media surveillance tool – and little is known of it. Retrieved from https://scroll.in/article/893015/40-government-departments-are-using-a-social-media-surveillance-tool-and-little-is-known-of-it

Shruthijith, K. (2009). Govt bans popular toon porn site. Retrieved from https://www.hindustantimes.com/entertainment/govt-bans-popular-toon-porn-site/story-M7UO7XgStS9Cfrvfziok6J.html

Singh, K. (2019). What porn ban? a 400% rise in vpn downloads in india shows where there's a will there's a way. Retrieved from https://qz.com/india/1759306/top-vpns-used-by-indians-to-watch-porn-despite-the-ban/

Singh, K. [Kushagra], Grover, G. & Bansal, V. (2020). How india censors the web. Retrieved from https://cis-india.org/internet-governance/blog/how-india-censors-the-web

Singh, M. [Manish]. (2019). Whatsapp reaches 400 million users in india, its biggest market. Retrieved from https://techcrunch.com/2019/07/26/whatsapp-india-users-400-million/

Singh, M. [Mausami]. (2017). Blue whale game: Rajya sabha chair directs government to take cognisance of 'suicide'. Retrieved from https://www.indiatoday.in/india/story/blue-whale-suicide-game-rajya-sabha-1027803-2017-08-03

Singh, O. (2019). Use of digital media in suicide prevention in adolescents and young adults. *Indian J of Psychiatry.* Retrieved from https://www.ncbi. nlm.nih.gov/pmc/articles/PMC6341923/

Singh, V. (2018). Anti-lynching measures: Social media sites to be held responsible. Retrieved from https://www.thehindu.com/news/national/anti-lynching-measures-panel-submits-report-to-rajnath-singh-led-group-of-ministers/article24812462.ece

Sneha Kalita v. Union of India. (2017). 2017 (13) SCALE 661.

Soni, Y. (2019). Parliamentary committee issues strict instructions to twitter on elections. Retrieved from https://inc42.com/buzz/parliamentary-committee-issues-strict-instructions-to-twitter-on-elections/

Special Correspondent. (2014). Insult to national anthem: Youth held. Retrieved from www.thehindu.com/todays-paper/tp-national/tp-kerala/insult-to-national-anthem-youth-held/article6336783.ece

Staff Reporter. (2018). Man live streams suicide on facebook. Retrieved from https://www.thehindu.com/news/cities/Delhi/man-live-streams-suicide-on-facebook/article24567463.ece

State of West Bengal v. Animesh Boxi. (2018). C.R.M. No. 11806 of 2017.

Statista. (2020). Leading countries based on number of facebook users as of october 2019. Retrieved from https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/

Subodh Gupta v. Herdsceneand. (2019). CS (OS) 483/2019.

S.Ve. Shekher v. Inspector of Police - Cyber Cell. (2018). 2018(2)KLT806.

Swami Ramdev v. Facebook. (2019). CS (OS) 27/2019.

Taneja, K. & Shah, K. M. (2019). The conflict in jammu and kashmir and the convergence of technology and terrorism. Retrieved from https://rusi.org/sites/default/files/20190807_grntt_paper_11.pdf

Tech2 News Staff. (2017). Blue whale challenge: Meity asks google, facebook, others to remove related links from their platforms. Retrieved from https://www.firstpost.com/tech/news-analysis/blue-whale-challenge-meity-asks-google-facebook-and-others-to-remove-links-related-to-this-game-from-their-platforms-3932813.html

Tehseen S Poonawalla v. Union of India. (2018). AIR 2018 SC 3354.

Telecom Regulatory Authority of India. (2019). *Telecom subscription data, august 2019.* Retrieved from https://main.trai.gov.in/sites/default/files/PR_No.101of2019.pdf

Tembhekar, C. (2018a). 'booze-on-call' busted, 50 shops lose licence. Retrieved from https://timesofindia.indiatimes.com/city/mumbai/booze-on-call-busted-50-shops-lose-licence/articleshow/65370844.cms

Tembhekar, C. (2018b). Excise department trains lens on those calling in for liquor. Retrieved from https://timesofindia.indiatimes.com/city/mumbai/excise-dept-trains-lens-on-those-calling-in-for-liquor/articleshow/65379663.cms

Thaker, A. (2019). Even tiktok is warning indians against election related fake news. Retrieved from https://qz.com/india/1593022/after-whatsapp-and-facebook-tiktok-fights-fake-news-in-india/

The Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications. (2017). 2018 (1) CTC 506.

The Wire Staff. (2019). Rapper hard kaur charged with sedition for posts against adityanath, bhagwat. Retrieved from https://thewire.in/rights/rapper-hard-kaur-charged-with-sedition-for-posts-against-adityanath-bhagwat

Times News Network. (2018). Agra youth live-streams suicide, 2,750 people watch but don?t call cops. Retrieved from https://rn.timesofindia.com/videos/news/agra-youth-live-streams-suicide-2750-people-watch-but-dont-call-cops/videoshow/64959823.cms

Tiwari, S. (2019). Petition in kerala high court seeks ban on telegram, cites terrorism and child porn. Retrieved from https://www.medianama.com/2019/10/223-kerala-hc-telegram-petition/

Tripathi, K. (2019). Rajeev chandrasekhar accuses social media platforms of bias, demands law to fix accountability. Retrieved from https://www.financialexpress.com/india-news/rajeev-chandrasekhar-accuses-social-media-platforms-of-bias-demands-law-to-fix-accountability/1647443/

UNESCO. (2018). Journalism, fake news and disinformation. Retrieved from https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

UNICEF. (2017). Faqs: Blue whale challenge - what parents need to know. Retrieved from http://www.unicef.in/STAYSAFEONLINE/Story-What-is-the-Blue-Whale-Challenge-and-why-should-parents-be-concerned-about-this-game-.html

Shreya Singhal v. Union of India. (2016). Supreme Court of India.

Vishwanath, A. (2018). Judges order lawyer's facebook account to be deleted for contempt of court. Retrieved from https://theprint.in/india/governance/himachal-pradesh-hc-orders-deletion-of-lawyers-facebook-account-for-contempt-of-court/106385/

Wire Staff. (2016). Contempt notice to ex-judge markandeya katju ignores supreme court's own rulings. Retrieved from https://thewire.in/law/supreme-court-notice-to-ex-judge-markandey-katju-ignores-valid-precedents

World Congress Against Sexual Exploitation of Children and Adolescents. (2008). *The rio de Janeiro declaration and call for action to prevent and stop sexual exploitation of children and adolescents.* Retrieved from https://www.unicef.org/protection/WCIII_Outcome_Document_Final.pdf

Youtube LLC v. Geeta Shroff. (2018). 2018 SCC OnLine Del 9439.

Acknowledgements

We thank participants at the Data Governance Network meeting of December 13, 2019, a blind reviewer, Smriti Parsheera and Renuka Sane for comments. All errors are our own.

About the Authors

The authors are technology policy researchers at the National Institute of Public Finance and Policy (NIPFP), New Delhi.

datagovernance.org dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork