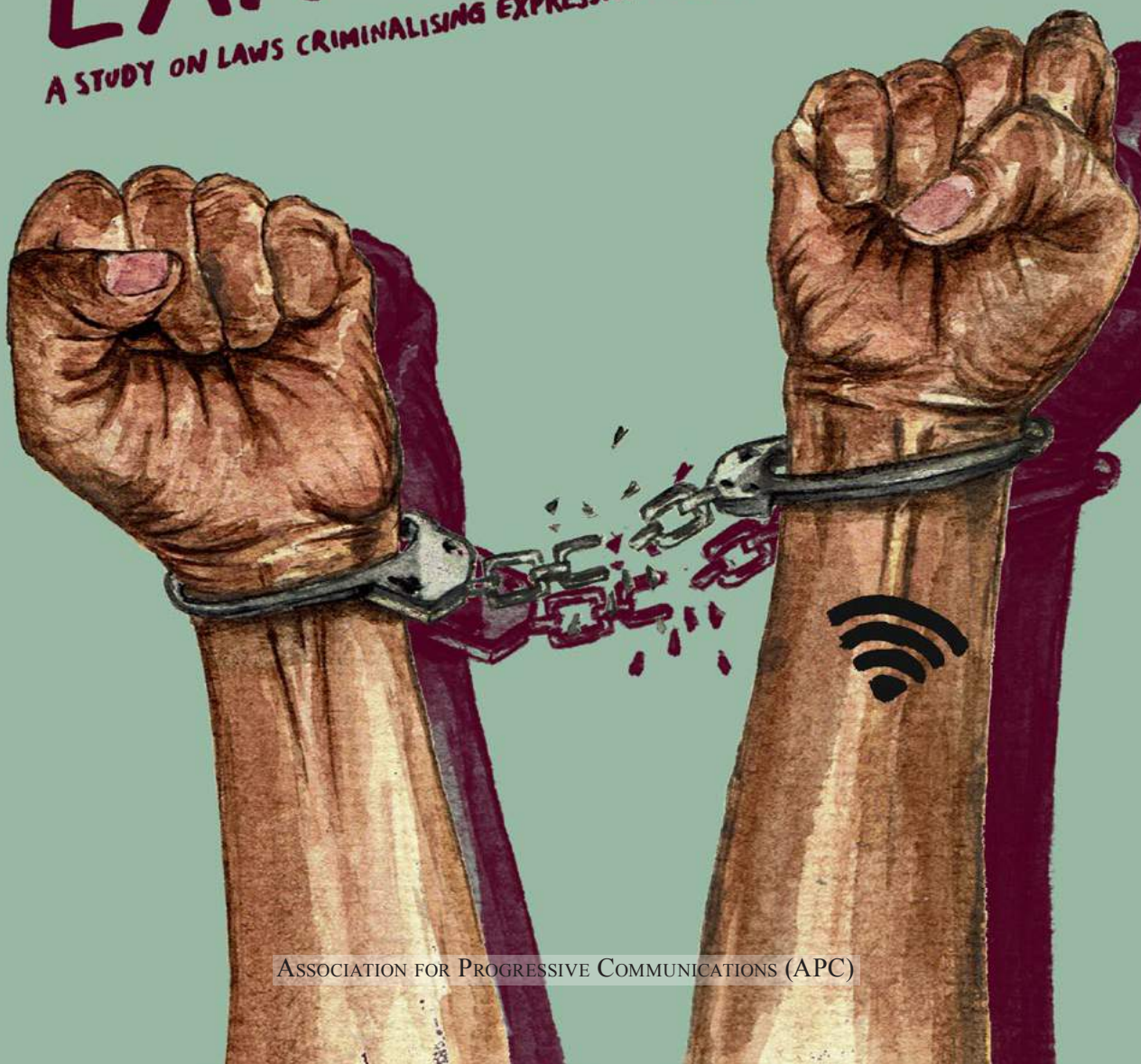
GISWatch 2017
SPECIAL EDITION

UNSHACKLING EXPRESSION:

A STUDY ON LAWS CRIMINALISING EXPRESSION ONLINE IN ASIA



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)

Annexure 6

Criminal law and freedom of expression on the internet in India

Anja Kovacs and Nayantara R
Internet Democracy Project

Introduction

In July 2017, a Muslim man was arrested in the South Indian city of Chennai on charges of sedition, on the basis of WhatsApp messages that he had received on his phone. One of the messages had called on people to protest at Jantar Mantar, New Delhi's officially designated protest site, against those who disrespected the Koran. The man was released after a magistrate found no evidence of anti-national activity or calls for violence.[1]

A few weeks later, on 8 August 2017, Indian internet users noticed that the Internet Archive, "a non-profit library of millions of free books, movies, software, music, websites, and more",[2] was no longer accessible in the country. Two days later, it emerged that internet service providers (ISPs) had taken down the page following a court order. The makers of two Indian films, *Jab Harry Met Sejal* and *Lipstick Under My Burkha*, had requested the court to block the Internet Archive as well as more than 2,600 file-sharing sites, in an effort to stop pirated copies of their films from being watched online.[3]

By the end of the month, the 47th internet shutdown of 2017 hit India – this time in the northern states of Haryana and Punjab. Mobile internet services were suspended because of growing tensions a day before a special court was to deliver its verdict in a rape case against high-profile godman[4] Gurmeet Ram Rahim Singh. The shutdown lasted six days. Internet lease lines were suspended in a smaller geographical area.[5] With four months left to go, India had already seen three times as many internet shutdowns in 2017 as in 2015.[6]

While the internet has often been hailed for its empowering impact on people's ability to express themselves, these incidents, recorded in a span of a mere six weeks, show that this potential can by no means be taken for granted. In India, as elsewhere, freedom of expression online is restricted in a number of ways. Focusing in particular on the criminalisation of freedom of expression but examining other barriers in law and policy as well, this report seeks to outline when and how laws in India are used to curtail the right to freedom of expression on the internet in ways that are overly broad.

The report consists of seven sections. Following this introduction, we will briefly discuss the methodology we have followed in researching and writing this report. For those not familiar with the Indian legal landscape, we will then describe the different types of law that affect the right to free speech and expression on the internet in India. Section four is the heart of this report and examines in detail the laws, policies and case laws that criminalise freedom of expression on the internet in India in ways that are overly broad. In section five, we analyse a number of other important threats to free speech online that further constitute the context in which the criminalisation of freedom of expression on the internet in India has to be understood – from government-mandated content restrictions to mass surveillance. Finally, we briefly highlight draft laws and policies which we believe give cause for concern over future violations of the right to freedom of speech and expression. We conclude the report with a summary and our conclusions.

1 Karthikeyan, D. (2017, 19 July). Arrest of Muslim Man for Receiving Phone Message Highlights Police Misuse of 'Sedition'. *The Wire*. https://thewire.in/159367/sedition-whatsapp-chennai-anti-national/

2 https://archive.org

3 Kelion, L. (2017, 9 August). Bollywood Blocks the Internet Archive. *BBC News*. http://www.bbc.com/news/technology-40875528

4 Godman is a colloquial term used in India for a type of charismatic guru. https://en.wikipedia.org/wiki/Godman_(India)

5 Indo Asian News Service. (2017, 27 August). Haryana, Punjab Suspend Mobile Internet Till Tuesday. *NDTV News*. http://www.ndtv.com/india-news/haryana-punjab-suspend-mobile-internet-till-tuesday-1742656

6 https://internetshutdowns.in; Pahwa, N. (2017, 28 August). Government of India issues rules for Internet Shutdowns. *Medianama*. https://www.medianama.com/2017/08/223-internet-shutdowns-india

Methodology

To research and write this report, we examined three different types of sources. First, we looked at all the laws and related rules that have an impact on freedom of expression online. Second, we considered case law in higher courts that has had a profound influence on the promotion and protection of the right to freedom of expression in India, including as it relates to the internet, or that has the potential to do so in the future. Finally, we also took into account media reports of charges booked by the police – even if those cases did not eventually result in a conviction – to be able to flag chilling effects, heckler's vetoes,[7] as well as implementation challenges.

We found that six grounds for restriction, in particular, are being used to criminalise free speech on the internet in ways that are not acceptable. These are defamation; sedition and the use of national symbols; contempt of court; hate speech; morality, obscenity and sexual expression; and intellectual property rights. In addition, we found five other legal and policy challenges relating to freedom of expression on the internet that are crucial to understand the broader landscape of digital censorship in India: government powers to block content; India's intermediary liability regime; the epidemic of network shutdowns in India; concerns around net neutrality; and digital surveillance in India. The substantive analysis of these challenges starts in the fourth section. However, for those not familiar with the Indian legal landscape, we want to first outline the different types of law that affect freedom of expression online in the country.[8]

Lay of the legal land

Legal foundations

The foundation for the freedom of speech and expression in India lies in Article 19(1)(a) of the Constitution of India, which states that all citizens shall have the right to freedom of speech and expression.

It was explicitly held in *Secretary, Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal*[9] that the right to freedom of speech and expression includes the right to impart and receive information via electronic media.

Article 19(2) lays down exceptions to this fundamental right. This sub-section identifies certain heads under which there may be reasonable restrictions to the freedom of speech and expression: the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

Laws that restrict freedom of speech and expression must be reasonable and fall within the contours of the subject matters listed in Article 19(2). Any legislation dealing with speech and expression on the internet can be challenged on the ground that it goes beyond the exceptions laid down in Article 19(2) of the Constitution.

Along with the right to equality (Article 14) and the right to life (Article 21), Article 19 forms the foundation for liberty and equality under the Constitution.

India's obligations towards the right to freedom of speech and expression also stem from being a signatory to the Universal Declaration of Human rights and the International Covenant on Civil and Political Rights (ICCPR).

The legislations that cover penal procedure and substantive law are the Code of Criminal Procedure, 1973, and the Indian Penal Code, 1860. The latter is a relic from the colonial period. These legislations continue to be used to book cases relating to speech on the internet as well.

Governance of online and networked spaces

Apart from the penal codes, the Information Technology Act, 2000 and the Amendment Act of 2008, as well as the rules framed under the Act, are other importants bases for the governance of electronic media, and consequently, for the criminalisation of speech and expression online.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, governs India's unique identity number project, which relies heavily on digital infrastructure and has ramifications not only for the right to privacy, but also for the right to freedom of speech and expression.

Legislations such as the Protection of Children from Sexual Offences Act, 2012, also specifically prohibit some forms of speech and expression on the internet. Other legislations, like the Contempt of Courts Act, 1971, the Prevention of Insults to National Honour Act, 1971, the Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989, and the Pre-Conception and Pre-Natal

7 In the strict legal sense, a heckler's veto occurs when the speaker's right is curtailed or restricted by the government in order to prevent a reacting party's behaviour. https://en.wikipedia.org/wiki/Heckler%27s_veto

8 Our outline of the Indian legal landscape draws on the five-category framework of laws and regulations that affect online freedom of expression, developed by SMEX.

9 Government of India v. Cricket Association of Bengal. 1995 AIR 1236.

Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994, do not specifically pertain to speech on electronic media, but they prohibit certain kinds of speech and are used to book charges against speech and expression on the internet as well.

Laws and policies on infrastructure

The Telecom Regulatory Authority of India (TRAI), established by the Telecom Regulatory Authority of India Act, 1997, has powers to regulate the telecommunications sector, with the mandate of protecting the interests of service providers and telecom subscribers while ensuring orderly growth of the sector. We will examine the connections between regulation of one aspect of this debate, that of network neutrality, and the right to freedom of speech and expression. Network neutrality is the principle that the internet is maintained as an open network, where network operators do not discriminate on the basis of origin or destination of traffic. Preserving network neutrality is central to making sure that the internet's potential of being a medium where freedom of speech and expression thrives can be realised.

Other laws

Laws on intellectual property rights (IPR) aim to strike a balance between protecting ownership and property rights, on the one hand, and not infringing on free speech, on the other. In copyright law, for example, fair use exceptions are forwarded as speech protecting where the public good is greater than the value derived from individual benefits of intellectual property. In the section on IPR, we look at the unique challenges that Indian laws on IPR pose to freedom of speech and expression.

Draft laws

Finally, a number of key bills and draft policies have been proposed on content and infrastructure regulation of electronic media which affect freedom of speech and expression. These include the Draft Prohibition of Indecent Representation of Women and Children Bill, 2012, the Draft Geospatial Information Regulation Bill, 2016, the Draft National Encryption Policy, 2015, and a forthcoming draft data protection policy. New provisions to address hate speech have been proposed as well, including to fill alleged gaps in the law that have emerged after the Supreme Court struck down as unconstitutional section 66A of the IT Act in 2015.[10]

10 Shreya Singhal v. Union of India. AIR 2015 SC 1523.

Criminalisation of online freedom of expression

Because of their far-reaching consequences for the speaker, criminal charges to restrict speech and expression can be a powerful tool of censorship.

Between 2009 and 2015, one provision of Indian law in particular became notorious for its chilling effect on freedom of expression online. Section 66A of the IT (Amendment) Act, 2008, provided for punishments for messages that were "grossly offensive", had a "menacing character" or were sent "for the purpose of causing annoyance or inconvenience," among other overly broad grounds. Following a slew of high-profile cases that involved abuse of the section, the provision's constitutionality was challenged in *Shreya Singhal v. Union of India*.[11] On 24 March 2015, the Supreme Court of India ruled that section 66A IT Act was "violative of Article 19(1)(a)" and could not be saved under Article 19(2), and struck down the provision in its entirety.

For those concerned with freedom of expression online in India, the verdict provided tremendous relief. But many challenges remain. For one thing, even following the Supreme Court's ruling, section 66A IT Act continues to be invoked by the police and lower courts.[12] In addition, freedom of expression online continues to be threatened through criminalisation in other ways that are not acceptable, on six grounds in particular: criminal defamation; sedition and the use of national symbols; contempt of court; hate speech; morality, obscenity and expressions of sexuality; and intellectual property rights.

What connects these different challenges is the deep influence of a concern for law and order in free speech jurisprudence in India. In particular, in *State of U.P. v. Lalai Singh Yadav,*[13] the Supreme Court upheld "ordered security" as a constitutional value, ensuring that where free speech and public order seem to clash, the latter is given precedence. Though there have been dissenting voices, this remains the dominant strand in free speech jurisprudence to this day and has led to a situation where, rather than the government having to ensure an environment in which everyone can speak freely, those who are speaking are expected to exercise

11 AIR 2015 SC 1523.

12 Mareedu, M. (2017, 8 April). Local court invokes annulled Sec 66A to convict a man. *New Indian Express*. www.newindianexpress.com/states/telangana/2017/apr/08/local-court-invokes-annulled-sec-66a-to-convict-a-man-1591308.html; Jha, A. (2016, 1 September). 2,000 Arrests In 12 Months, 3,000 In Just 3? How Cops Use 66A Even After SC Scrapped It. *Youth Ki Awaaz*. https://www.youthkiawaaz.com/2016/09/66a-it-act-ncrb-crime-statistics

13 AIR 1977 SC 202.

caution lest anyone gets outraged. Even truth is not accorded the same value as order.[14]

In what follows, we examine relevant laws, case law and cases for each of the grounds mentioned above in detail. It is against the background of the precedence of order over speech that these analyses have to be read.

Defamation

Both civil and criminal remedies exist in Indian law for someone aggrieved of defamation, one of the eight exceptions to Article 19(1)(a) mentioned in the Constitution. Under the un-codified civil law remedy, one can obtain injunctive orders and/or claim damages for the publication of allegedly defamatory material. The criminal remedy to defamation, codified in sections 499 and 500 of the Indian Penal Code (IPC), punishes the crime with imprisonment and fines. Depending on the outcome desired, parties file for either a civil or criminal remedy, or for both. What is common among the two types of remedies is that they are routinely used by powerful players to strong-arm critics into silence.

The civil remedy is often used to obtain injunctive orders in the absence of respondents to the case, in addition to huge sums of money, as damages. Most recently, Baba Ramdev, a godman, politician and businessman, got an ex parte injunction against Juggernaut publishers, Flipkart and Amazon, stopping them from distributing a biography of him by Priyanka Pathak-Narain, on the grounds of it being defamatory.[15] In another recent case, Member of Parliament Rajeev Chandrashekhar was seeking to prevent online news media outlet The Wire from publishing two stories about him that had a very clear public interest angle.[16] The City Civil Court of Bangalore passed an ex parte order for temporary injunction against publication of the two articles, which highlighted the conflicts of interest between the political roles Chandrashekhar holds, on the one hand, and his investments in defence manufacturing firms and the news media outlet Republic TV, on the other. There are numerous such instances of ex parte injunctions that have been obtained in order to silence the publishing of material on the internet as well as in print media.[17]

The criminal remedy is especially useful for purposes of intimidation by politicians, actors, corporations and other powerful entities, as the offence is punishable with jail time and not just payment of monetary damages. The offence is bailable, non-cognisable and compoundable.

Sections 499 and 500 read as follows:[18]

> 499. Defamation.—
> Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.
> Explanation 1.—It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.
> Explanation 2.—It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
> Explanation 3.—An imputation in the form of an alternative or expressed ironically, may amount to defamation.
> Explanation 4.—No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.
> 500. Punishment for defamation.—
> Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

The asymmetry of power between those who bring the charges and those who are charged for defamatory speech on the internet is frequently steep in

14 Law Commission of India. (2017). *Report 267 Hate Speech*. New Delhi: Law Commission. www.lawcomssionofindia.nic.in/reports/Report267.pdf; Narrain, S. (2016). Hate Speech, Hurt Sentiment, and the (Im)Possibility of Free Speech. *Economic and Political Weekly*, *51*(17). http://www.epw.in/journal/2016/17/special-articles/hate-speech-hurt-sentiment-and-impossibility-free-speech.html

15 IANS. (2017, 11 August). Juggernaut restrained from distributing book on Ramdev, says will appeal. *Indian Express*. www.indianexpress.com/article/india/juggernaut-restrained-from-distributing-book-on-ramdev-says-will-appeal-4792196

16 Scroll. (2017, 7 March). In highly unusual move, Bengaluru court orders The Wire to remove articles on Rajeev Chandrasekhar. *Scroll*. www.scroll.in/article/831159/in-highly-unusual-move-bengaluru-court-orders-the-wire-to-remove-articles-on-rajeev-chandrasekhar

17 Scroll. (2017, 17 October). 'Attempt to gag': The Wire criticises injunction against it in Jay Shah defamation case. *Scroll*. https://scroll.in/latest/854371/attempt-to-gag-the-wire-criticises-injunction-against-it-in-jay-shah-defamation-case

18 The illustrations and exceptions text in the section have not been included, in the interest of space.

the case of criminal defamation charges as well. For example, the Adani group issued a legal notice for criminal and civil defamation against media house The Wire for republishing an article that originally appeared in Economic and Political Weekly (EPW), titled "Modi Government's 500 Crore Bonanza to Adani Group Company", in June 2017. EPW also received a similar legal notice a few days later, in July. Bollywood actor Aamir Khan filed a defamation suit against a person for making comments against the actor's show *Satyameva Jayate* on social media.[19] And in another exemplary case of intimidation, a law student received a legal notice for charges of criminal and civil defamation for publishing a blog post on ongoing trademark litigation between the Financial Times Ltd. and Times of India.[20] Ironically, a media house was on the other side of the fence, issuing the legal notice.

A batch of petitions, including most prominently those by politicians Arvind Kejriwal, Subramanian Swamy and Rahul Gandhi, challenged the constitutionality of criminal defamation in the Supreme Court. The petitions contended that sections 499 and 500 IPC, and section 199(1) to 199(4) of the Code of Criminal Procedure, which lay down the procedure for prosecution for defamation, go beyond the reasonable restrictions to the right to freedom of speech and expression under Article 19(2). The petitions also held that the civil remedy of defamation is sufficient for safeguarding the right to reputation under Article 21 of the Constitution. In a case known by the name of one of the petitions, *Subramaniam Swamy v. Union of India,*[21] the Supreme Court took up these petitions together to decide on the constitutionality of the criminal defamation provisions.

That the criminal remedy goes beyond the "reasonable" restrictions under Article 19(2) was argued on many grounds, which often sought to differentiate the criminal remedy from the civil remedy.[22] For example, in contrast to the civil remedy, the criminal remedy involves the complainant bearing little costs, as state resources are spent on prosecuting the accused, to protect individual rights. This leads to greater chances of frivolous complaints being filed. In addition, the burden placed on the accused and the criminal nature of the complaint allows for harassment at the hands of the persons filing charges.

Ruling on the petitions, the Supreme Court of India paid lip service to the fundamental right to freedom of speech and expression and international covenants – before deciding that the sections were indeed not unconstitutional. Going against a global push away from criminal remedies for defamation, the Court ruled that there was a need to balance the right to reputation, which is part of the fundamental right to life, and therefore, the remedy of criminal defamation was a *reasonable* restriction under Article 19(2). This judgment of the Supreme Court received flak from many commentators for its regressiveness in free speech jurisprudence, for being needlessly wordy, and for not engaging satisfactorily with the arguments of petitioners.[23]

Criminal defamation and publication on the internet

If the petitioners sought to distinguish the criminal from the civil remedy in *Subramaniam Swamy v. Union of India,* so, reportedly, did the Ministry of Home Affairs, albeit for a different reason: according to a news report, the Ministry submitted to the Supreme Court that because of the emergence of new technology, the criminal remedy is, in fact, required:[24]

> Civil remedy for defamation is not efficacious remedy per se. The civil remedies on an average take longer than criminal remedies. Furthermore, with the advent of new forms of technology, acts like online defamation cannot be adequately countered by means of civil remedies.

It is unclear on what grounds the government sought to create a distinction between "online defamation" and its print or broadcast counterpart. The ease of publication, the speed of transmission of statements, along with its duplicability seems to be the implicit basis for the distinction. However, this argument begs the question: are restrictions to free speech then to be higher for print media outlets that have a digital edition?

19 India Today. (2014, 19 April). Retired merchant navy officer Ajit Vadakayil arrested for defaming actor Aamir Khan. *India Today.* http://indiatoday.intoday.in/story/aamir-khan-man-held-from-karnataka-for-defaming-actor-aamir-khan/1/356626.html

20 Reddy, P. (2013, 21 May). The Times Publishing House threatens to sue our blogger for alleged defamation – we ain't going down without a fight! *Spicy IP.* https://spicyip.com/2013/05/the-times-publishing-house-threatens-to.html

21 WP (Crl) 184 of 2014.

22 Thomas, A. L. (2016, 27 May). Subramanian Swamy v. UoI: Unanswered Arguments. *Legally India*. https://www.legallyindia.com/blogs/subramanian-swamy-v-uoi-unanswered-arguments

23 Acharya, B. (2016, 14 May). Criminal Defamation and the Supreme Court's Loss of Reputation. *The Wire*. https://www.thewire.in/36169/criminal-defamation-and-the-supreme-courts-loss-of-reputation

24 Mishra, P. (2015, 12 July). Online defamation cannot be countered by civil remedies, Centre tells Supreme Court. *DNA News*. http://www.dnaindia.com/india/report-online-defamation-cannot-be-countered-by-civil-remedies-centre-tells-supreme-court-2103811

Whether "new forms of technology" merit different treatment or not is not further discussed in the order of the Court in *Subramaniam Swamy v. Union of India*. However, the same court in 2009 had made statements that indicated that defamation on the internet had different effects, and therefore merited harsher consequences. In that case, a 19-year-old blogger was arrested for creating a group ("community") on social media site Orkut, that was allegedly defamatory to the political party Shiv Sena. The Supreme Court refused to quash the criminal proceedings against the boy and argued that restrictions to free speech on the internet should be higher. The judge noted that "any blogger posting material on the web should be aware of the reach of the internet and hence also be willing to face the consequences of such action."[25]

In a 2010 civil defamation suit, *Tata Sons Limited. v. Greenpeace International & Anr.*,[26] the Supreme Court made slightly different observations as to when it would be relevant that the publication of allegedly defamatory statement is made on the internet.

In this case, the petitioners moved the Court for a permanent injunction against Greenpeace along with damages for defamation under the civil remedy and trademark infringement. The facts of the case were that Tata Sons Limited was suing Greenpeace International, a not-for-profit organisation, for releasing a videogame through which it sought to publicise the harms that Tata Sons' business ventures would wreak on endangered olive ridley turtles.

The creators of the game defended their actions on the grounds of freedom of speech and exceptions under section 29(4) of the Trade Marks Act, 1999, which allows for the use of a trademark for criticism, fair comment and parody if it is with due cause. The Tata Group prayed for an injunction on the grounds that, as the "publication" happened on the internet, the likelihood of injury was greater if the injunction were refused, and that this should be a consideration for the court as it balanced convenience and irreparable hardship. According to the Tata Group, the damage to its reputation was "continuing and spreading every minute that the game stays online," and as a result, an injunction should be granted.

The Court ruled, however, that the nature of the medium of the internet may only be a consideration in assessment of damages. The Court held that the term "publication" encompassed all forms and mediums, including the internet:

> That an internet publication has wider viewership, or a degree of permanence, and greater accessibility, than other fixed (as opposed to intangible) mediums of expression does not alter the essential part, i.e. that it is a forum or medium.

In discussing the Canadian case relied upon by the petitioners, the Court drew attention to the detail that even in that case, a different standard for libel was not mooted for publication on the internet, and "suspected" that such a distinction (between the internet and other forms of publication) is not constitutionally sanctioned:

> Formulating and adopting any other approach would result in disturbing the balance between free speech and the interest of any individual or corporate body in restraining another from discussing matters of concern, so finely woven in the texture of the Bonnard ruling.

Publication and republication in the digital age

Another matter to consider in the age of the internet is what constitutes "making or publishing imputations". According to section 499 of the IPC, the offence of criminal defamation would be committed if one "makes or publishes any imputation concerning any person [...] to defame that person."

Union Minister Arun Jaitley filed a criminal defamation complaint in December 2015 against the Chief Minister of Delhi, Arvind Kejriwal, for publishing a tweet that Jaitley alleges to be defamatory. He also arraigned a number of others who retweeted Kejriwal's original tweet, including the Aam Aadmi Party's Raghav Chaddha. Chaddha approached the Supreme Court to seek a direction that a retweet cannot form the basis of a criminal prosecution. The Supreme Court has directed the Delhi High Court to look into the matter. As noted by Devika Agarwal,[27] republishing a defamatory article constitutes defamation according to interpretation by Indian courts.[28] It remains to be seen whether a retweet will be considered as "publishing" by the Delhi High Court.

In the case of *Khawar Butt v. Asif Nazir Mir,*[29] the plaintiffs instituted a civil suit for defamation

25 Liang, L. (2009, 25 February). Bloggers and Defamation. *Kafila*. http://www.kafila.online/2009/02/25/bloggers-and-defamation

26 CS(OS) 1407/2010.

27 Agarwal, D. (2017, 25 September). Arun Jaitley's suit against AAP's Raghav Chadha: Does republishing of defamatory content amount to 'defamation'? *FirstPost*. www.firstpost.com/politics/arun-jaitleys-suit-againt-aaps-raghav-chadha-does-republishing-of-defamatory-content-amount-to-defamation-4058989.html

28 Re: EVK Sampath, AIR 1961 Mad 318.

29 CS (OS) 290/2010.

for republishing print material on Facebook. The question before the Delhi High Court was whether republication on the internet constituted a fresh offence, and whether the limitation period would begin afresh with the republishing. Arguing that the post on Facebook qualified as a fresh offence, and the suit cannot be barred by limitation, the plaintiffs sought to distinguish the internet as a medium from print on the ground that "a publication on a website can voluntarily be withdrawn by the publisher, unlike publication in print media, which, once published cannot be withdrawn."

This is only true, however, in so far as it does not consider archived versions of many websites. The Delhi High Court held against the plaintiffs, by holding against the Multiple Publication Rule:

> I am of the view that the Single Publication Rule is more appropriate and pragmatic to apply, rather the Multiple Publication Rule. I find the reasoning adopted by the American Courts in this regard to be more appealing than the one adopted by the English Courts, prior to the amendment of the law by the introduction of the Defamation Act, 2013. It is the policy of the law of limitation to bar the remedy beyond the prescribed period. That legislative policy would stand defeated if the mere continued residing of the defamatory material or article on the website were to give a continuous cause of action to the plaintiff to sue for defamation/libel. Of course, if there is re-publication resorted to by the defendant-with a view to reach the different or larger section of the public in respect of the defamatory article or material, it would give rise to a fresh cause of action.

If the Court would not have held in favour of the Single Publication Rule, it would have been possible for a plaintiff to sue for every "hit" of the webpage.

Free speech online and the truth defence

One of the main issues with criminal defamation has been the burden placed on the accused, as truth is not a defence in itself without the accompanying requirement, noted in exception 1, of being in the public interest. This disproportionate burden creates a massive chilling effect on speech and expression on the internet. As noted by Shehla Rashid Shora and Anja Kovacs, explanation 2 to section 499, for example, could arguably be drawn on to penalise the authors of bad reviews given to products or services on the internet.[30] In the age of e-commerce and internet-mediated service delivery, such provisions can prove to be highly problematic for citizen journalists who, using only a cell phone and an internet connection, seek to expose shady business practices.

This is particularly noteworthy as corporations continue to be able to file complaints of criminal defamation. In 2014, Mahan Coal Limited, a corporation, filed a complaint against environmental rights campaigner Priya Pillai for allegedly defamatory remarks made by her.[31] Her comments in a blog post questioning the speedy clearance of projects by the environment minister, benefitting corporations like the Essar Group at the expense of the forests, people and wildlife, were among the things that irked Mahal Coal Limited, a company promoted by ventures of the Essar Group.

Pillai filed a petition challenging the provisions of criminal defamation, along with challenging the ability of corporations to file criminal defamation complaints. The Supreme Court in *Subramaniam Swamy v. Union of India* locates the right to reputation under the right to life and personal liberty in Article 21, which is not a right available to corporations. Yet, a two-judge bench of the Supreme Court disposed of Pillai's petition, in the aftermath of the judgment in *Subramaniam Swamy v. Union of India,* saying nothing remained to be discussed.

Looking forward

In response to the misuse of the section by powerful actors to intimidate and chill free speech, the Supreme Court in *Subramaniam Swamy v. Union of India* unfortunately held that "an abuse of process or the potential for abuse of a law is no ground for repealing the law itself." As noted by Lawrence Liang, a solution to eliminating maliciousness may be to use more frequently the power of the courts under Section 250 of the Criminal Procedure Code, which provides for "compensation for accusation without reasonable cause."[32]

A private member's bill has been presented to the Parliament by Member of Parliament Tathagatha Satpathy to repeal provisions on criminal defamation and codify the civil remedy to defamation.[33] It would be heartening if the Parliament ups its record of standing up for free speech, as the Supreme Court has in this instance failed to uphold citizens' rights.

30 Shora, S. R., & Kovacs, A. (2013). *Criminalising Dissent? An Analysis of the Application of Criminal Law to Speech on the Internet through Case Studies*. New Delhi: Internet Democracy Project.

31 Parthasarathy, S. (2016, 1 November). Blocked Out. *Caravan Magazine*. www.caravanmagazine.in/perspectives/blocked-out-corporations-defamation

32 Liang, L. (2009, 25 February). Op. cit.

33 See https://speechbill.in

Sedition and national symbols

> Section 124A of the IPC concerns sedition:
> Section 124A.—
> Whoever, by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with imprisonment for life, to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine.
> Explanation 1.—The expression "disaffection" includes disloyalty and all feelings of enmity.
> Explanation 2.—Comments expressing disapprobation of the measures of the Government with a view to obtain their alteration by lawful means, without exciting or attempting to excite hatred, contempt or disaffection, do not constitute an offence under this section.
> Explanation 3.—Comments expressing disapprobation of the administrative or other action of the Government without exciting or attempting to excite hatred, contempt or disaffection, do not constitute an offence under this section.

The colonial origins of Indian sedition law, its role in the independence struggles and its chequered history in the post-independence era are all well recorded.[34] In the last few decades, there has been strong speech-protecting jurisprudence in the courts when it comes to interpretation of the provisions on sedition: the objective criteria of "incitement"[35] to "imminent"[36] "violence" are required to be present for any speech to be curtailed. However, in practice, especially on the internet, we see a stark difference between law and implementation where sedition is concerned. Several trends deserve to be highlighted.

First, all too often the police book charges of sedition for speech and expression on the internet that very obviously does not meet the criteria under the section. For example, as mentioned earlier, according to news reports a man in Chennai was booked under section 124A for receiving an "anti-national" message on WhatsApp.[37] The alleged "anti-national" message was a voice note in Urdu, calling for a protest, but was nowhere close to inciting violence, let alone imminently. In Badaun, an individual was arrested for posting the caption "I love Pakistan" along with his picture.[38] Even a former judge of the Supreme Court has not been spared: Justice Markandey Katju was booked for sedition under section 124A for saying in a Facebook post that Pakistan can take Kashmir if it agrees to take Bihar too.[39]

Second, phrases that gain currency on social media and subsequently in wider parlance, but that have no legal standing, become an informal lexicon to justify sedition charges. For example, "anti-national", which is neither a category defined under the section of sedition nor punishable under any legislative provision, is a term often used to refer to persons ostensibly liable for sedition, and is frequently bandied about in the filing of charges. Thus, in August 2016, a man was arrested and remained in judicial custody for several days for "liking, sharing and forwarding anti-India posts" on Facebook. The first information report (FIR)[40] reads:

> An anti-national post, in which India is represented as a mouse swept away by a broom, has been brought to notice. [It] asks for freedom for Kashmiris and has the flags of Pakistan and China. It is shown that some people have black flags and black bands across their faces and are asking for Kashmir's freedom.[41]

Third, there have been cases in which electronic media evidence was manipulated to make a case for sedition. For example, students of Jawaharlal Nehru University (JNU), New Delhi, were arrested for allegedly shouting slogans considered seditious during a protest meeting to mark the anniversary of the death of a separatist leader who was hanged. A

34 Dev, A. (2016, 25 February). A History of the Infamous Section 124A. *The Caravan*. www.caravanmagazine.in/vantage/section-124a-sedition-jnu-protests; Liang, L. (2016. 13 February). A Short Summary of the Law of Sedition in India. *The Wire*. https://www.thewire.in/21472/a-short-summary-of-the-law-of-sedition-in-india

35 Shreya Singhal v. Union of India. AIR 2015 SC 1523.

36 Arup Bhuyan v. State of Assam. (2011) 3 SCC 377.

37 Pathak, P. (2017, 20 July). Chennai man arrested for receiving anti-national WhatsApp message. Yes, for receiving it. *India Today*. www.indiatoday.intoday.in/technology/story/chennai-man-arrested-for-receiving-anti-national-whatsapp-message-yes-for-receiving-it/1/1005622.html

38 Press Trust of India. (2017, 8 August). Badaun man booked for sedition for his 'I support Pakistan' Facebook post. *Times Now*. www.timesnownews.com/india/article/badaun-man-booked-for-sedition-for-his-i-support-pakistan-facebook-post/70657

39 The Wire. (2016, 28 September). Markandey Katju Faces Sedition Charge for Facebook Post about Bihar. *The Wire*. https://thewire.in/69547/markandey-katju-faces-sedition-charge-for-facebook-post-about-bihar/

40 In criminal law, the first information report (FIR) is a report that provides information first in point of time about a crime. https://www.lawnotes.in/First_Information_Report

41 Ghose, D. (2016, 6 August) Kashmiri held for sedition: Chhattisgarh cops probe who made 'anti-India' FB post. *Indian Express*. www.indianexpress.com/article/india/india-news-india/kashmiri-held-for-sedition-chhattisgarh-cops-probe-who-made-anti-india-fb-post-2956483

forensic probe later found that two of the seven videos on the basis of which arrests were made were in fact doctored.[42] In a separate incident of arrest of college students on charges of sedition, the Metropolitan Magistrate hearing the case said that the authenticity of the videos should be determined before the filing of an FIR.[43]

But even if the contents of the videos of the JNU protests were known to be true, the speech in question would still not qualify as seditious.[44] It is established law in *Balwant Singh v. State of Punjab*[45] that raising separatist slogans once or twice by a few individuals does not amount to exciting or aiming to excite hatred or disaffection towards the government. In the landmark judgment of *Shreya Singhal v. Union of India,* the Supreme Court required that one differentiate between "advocacy" and "incitement" of violence, and that only the latter is punishable. Yet, across the country, public opinion continues to be mobilised around such doctored videos and police continue to book charges and arrest persons for the most innocuous of speech.

The misapplication of the section does not stop with the arrest of those making the speech, but bizarrely, extends even to those receiving it. For example, a WhatsApp group administrator was arrested in Karnataka for receiving a message insulting the prime minister.[46] Or in some cases, charges are brought against "unknown persons": Haryana police filed an FIR against "unknown persons" for a message shared on WhatsApp on the topic of the Jat agitation, which was "provoking".[47]

It is common for the sedition provision to be used in conjunction with the Prevention of Insults to National Honour Act, 1971, to arrest persons even when no offences are made out. Section 2 of the Prevention of Insults to National Honour Act, 1971 states that:

> Whoever in any public place or in any other place within public view burns, mutilates, defaces, defiles, disfigures, destroys, tramples upon or otherwise shows disrespect to or brings into contempt (whether by words, either spoken or written, or by acts) the Indian National Flag or the Constitution of India or any part thereof, shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

Thus, a student was arrested in Kerala for altering the lyrics of the national anthem in a Facebook post and "insulting" India, in addition to refusing to stand up for the national anthem.[48] Another man, a writer, was taken into custody for a similar charge of showing disrespect to the national anthem in his book and in a Facebook post, in December 2016 – he was booked for sedition.[49] In an atmosphere of heightened performative nationalism, these legislations are seeing more use to target political speech on social media.

Common Cause, a not-for-profit organisation, observing widespread misuse of the sedition section, filed a writ petition in the Supreme Court.[50] The petition notes that according to the National Crime Records Bureau (NCRB) Report, 2014, 47 sedition cases were reported in the year across nine states; many of these cases did not satisfy the prerequisite of incitement of violence. Of the 58 people arrested for sedition, only one person was convicted. The figures continue to be similarly abysmal for 2015, the last year for which NCRB data is available as of the time of writing. Responding to a question raised in the Lok Sabha, the government said that 35 cases of sedition were registered across the country in 2016.[51]

The petition filed by Common Cause asked for the issuance of an appropriate writ, order or direction requiring certification from the Director General of Police or Commissioner of Police that the alleged seditious act either led to incitement of violence or had the tendency or intention to create public disorder, before the filing of an FIR. The Court issued an order that criticism against the government does not constitute sedition, but did not see it "necessary" to issue more specific directions.[52]

42 Das, B. (2016, 19 February). Forensic experts say Kanhaiya video was doctored. *IndiaToday*. www.indiatoday.intoday.in/story/forensic-experts-say-kanhaiya-video-was-doctored/1/600808.html

43 Press Trust of India. (2017, 29 August). Ramjas College Ruckus: Can't Press Sedition on Basis of Unathenticated Videos, Says Delhi Court. *News 18*. www.news18.com/news/india/ramjas-ruckus-cant-press-sedition-on-basis-of-unathenticated-videos-says-court-1504375.html

44 Ibid.

45 1995 (1) SCR 411.

46 Express News Service. (2017, 3 May) Karnataka: WhatsApp group admin in jail over PM Narendra Modi post. *Indian Express*. www.indianexpress.com/article/india/karnataka-whatsapp-group-admin-in-jail-over-pm-narendra-modi-post-4638071/

47 Narrain, S., & Seshu, G. (2016, 19 August). Sedition goes viral. *The Hoot*. http://www.thehoot.org/free-speech/media-freedom/sedition-goes-viral-9578

48 The Hindu. (2014, 21 August). Insult to national anthem: Youth held. *The Hindu*. www.thehindu.com/todays-paper/tp-national/tp-kerala/insult-to-national-anthem-youth-held/article6336783.ece

49 Hindustan Times. (2016, 19 December). Kerala writer Chavara, held for 'insulting national anthem', on fast. *Hindustan Times*. www.hindustantimes.com/india-news/arrested-kerala-writer-on-fast-seeking-withdrawal-of-sedition-case/story-7Uap5YaSugKiuY6VTdtmSO.html

50 Common Cause and Anr. v. Union of India. WP (Civil) 683 of 2016.

51 Press Trust of India. (2017, 1 August). 35 sedition cases registered in 2016, govt tells Lok Sabha. *Hindustan Times*. http://www.hindustantimes.com/india-news/35-sedition-cases-registered-in-2016-govt-tells-lok-sabha/story-k5HUAkOZoHsYnCA30Z5A2H.html

52 Venkatesan, J. (2016, 5 September). Supreme Court Warns Police That Criticism of Government Is Not Sedition. *The Wire*. https://thewire.in/64281/criticism-of-government-does-not-constitute-sedition-says-supreme-court

Contempt of court

Contempt of court is one of the exceptions mentioned in Article 19(2) of the Constitution. The Contempt of Courts Act, 1971, is the legislation which details what may be considered an offence. The civil offence of contempt is defined in section 2(b) as "wilful disobedience to any judgment, decree, direction, order, writ or other process of a court or wilful breach of an undertaking given to a court."

The criminal offence of contempt is defined in section 2(c) as:

> The publication (whether by words, spoken or written, or by signs, or by visible representation, or otherwise) of any matter or the doing of any other act whatsoever which
> (i) scandalises or tends to scandalise, or lowers or tends to lower the authority of, any court; or
> (ii) prejudices, or interferes or tends to interfere with, the due course of any judicial proceeding; or
> (iii) interferes or tends to interfere with, or obstructs or tends to obstruct, the administration of justice in any other manner.

Cases on contempt of court related to the internet are mostly filed under the criminal offence section, as the civil offence pertains to simple wilful disobedience towards a specific direction given by a court. As pointed out by constitutional scholar Gautam Bhatia,[53] the section on the criminal offence of contempt can be interpreted either to mean that subsections (i), (ii) and (iii) have to be fulfilled, or that if merely sub-section (i) is fulfilled, the offence is made out. The court has over the years favoured the latter interpretation. There is no requirement that such scandalising or tendency to scandalise has to prejudice, interfere with or obstruct the administration of justice. The court has also not provided any guidelines to determine what constitutes scandalising the courts.

This has led to charges being filed for, among others, content that is criticism of judgment. For example, a man was sentenced to a month's jail time for "not only making scandalous statements against the judiciary, but also posting them on social networking websites"[54] – as if the latter action compounds the offence. In this case, the accused had simply made statements to the effect that he had lost faith in the judiciary, after a dispute over real estate was not working out in his favour. Similarly, a notice of contempt was sent to a former judge of the Supreme Court, Justice Katju, after he criticised the Supreme Court for its judgment on a case of rape and murder. The charges against the former judge were dropped after he delivered an apology.[55] In February 2017, the Bombay High Court issued a suo moto order against comments made by a person in a Facebook post against the court's order banning cell phones within the courtroom.[56] This is criticism of a policy of the Court which has implications for access to judicial process and, arguably, to justice.

Parody is affected as well. For example, "Bombay High Court" is a parody account on Facebook, offering a humorous take on goings-on in the Court. The creator of this account is reported to have been threatened for contempt.[57] According to a news report, the Ministry of Law and Justice similarly forwarded a complaint about certain Facebook pages to the Secretary General of the Supreme Court and the Registrar General of the Delhi High Court, with a request to take "further appropriate action". The complaint concerned satirical pages carrying the names of the Supreme Court and Delhi High Court: the pages were allegedly posting defamatory and contemptuous content that showed the judges and the judiciary in a poor light.[58]

In still another instance, the Bombay High Court, in response to a petition filed by the Bombay Bar Association and the Advocates Association of Western India, ordered the takedown of videos of court proceedings on YouTube and directed YouTube to not allow such content to be posted.[59] This raises issues of intermediary liability, apart from whether criticism of the court's orders itself is enough to "scandalise" a court.

53 Bhatia, G. (2016). *Offend, Shock, or Disturb. Free Speech under the Indian Constitution*. New Delhi: Oxford University Press.

54 Mumbai Mirror. (2014, 2 December). Man gets one month in jail for contempt of court. *Mumbai Mirror*. www.mumbaimirror.indiatimes.com/mumbai/crime//articleshow/45342096.cms

55 Indian Express. (2017, 6 January). Supreme Court accepts Justice Markandey Katju's apology, closes contempt proceedings. *Indian Express*. www.indianexpress.com/article/india/justice-markandey-katju-tenders-unconditional-apology-to-supreme-court-4461887

56 Chaudhari, K. (2016, 23 February). Facebook may face contempt motion in case on secretly shot Bombay high court video. *Hindustan Times*. www.hindustantimes.com/mumbai-news/facebook-may-face-contempt-motion-in-case-on-secretly-shot-bombay-high-court-video/story-vhuYUU20QSBYUSzlhkQ2JK.html

57 Shukla, A. (2016, 31 December). Meet the man behind 'Bombay High Court' parody account on Facebook. *Midday*. www.mid-day.com/articles/meet-man-behind-bombay-high-court-parody-account-on-facebook-mumbai-news/17873159

58 Nair, H. (2016, 23 January). Centre presses dislike on anti-court facebook pages. *India Today*. www.indiatoday.intoday.in/story/centre-presses-dislike-on-anti-court-facebook-pages/1/577672.html

59 Ibid.

Hate speech

India has a number of provisions on its books that seek to restrict speech that can negatively affect the relations between its diverse communities, hurt their religious feelings, or prejudice their integration into the national community. In light of India's size and diversity, it is quite understandable that the country's laws contain a number of provisions aimed at ensuring the peaceful coexistence of its peoples. In practice, however, the way in which some of these provisions in the Indian Penal Code in particular have been phrased and interpreted leads to easy misuse, and may well harm the relations between India's communities rather than helping them.

Among the sections in the Indian Penal Code that are frequently used to restrict freedom of expression online,[60] the wording of sections 153A and 505(2) IPC is quite similar:

> 153A. Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.— (1) Whoever—
> (a) by words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities [...] shall be punished with imprisonment which may extend to three years, or with fine, or with both.
> 505(2) Statements creating or promoting enmity, hatred or ill-will between classes.—
> Whoever makes, publishes or circulates any statement or report containing rumour or alarming news with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities, shall be punished with imprisonment which may extend to three years, or with fine, or with both.

Similarly, sections 295A and 298 IPC, too, resemble each other:

> 295A. Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs.—
> Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India, by words, either spoken or written, or by signs or by visible representations or otherwise, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
> 298. Uttering, words, etc., with deliberate intent to wound the religious feelings of any person.—
> Whoever, with the deliberate intention of wounding the religious feelings of any person, utters any word or makes any sound in the hearing of that person or makes any gesture in the sight of that person or places, any object in the sight of that person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

Under section 196 of the Code of Criminal Procedure, a court cannot take cognisance of a case under sections 153A or 295A without the previous sanction of the central government or state government. Before according sanction, the central government or state government may order a preliminary investigation by a police officer not being below the rank of inspector.

Perhaps the most notorious example of misuse of these sections is from November 2012, when a young woman, Shaheen Dada, was arrested for a Facebook post she wrote questioning the shutdown of Mumbai that followed the death of Bal Thackeray, the founder of the Shiv Sena. The Shiv Sena is a right-wing ethnocentric party with a particularly strong following in Mumbai. Following its leader's death, businesses throughout the city had been forced to shut and taxis went off the roads, all under the threat of violence. Shaheen Dada wrote:

> With all respect, every day, thousands of people die, but still the world moves on. Just due to one politician died a natural death, everyone just goes bonkers. They should know, we are resilient by force, not by choice. When was the last time, did anyone showed some respect or even a two-minute silence for Shaheed Bhagat Singh, Azad, Sukhdev or any of the people because of whom we are free-living Indians? Respect is earned, given, and definitely not forced. Today, Mumbai shuts down due to fear, not due to respect.[61]

60 For a more complete overview of hate speech provisions in Indian law, see Law Commission of India. (2017). Op. cit.

61 Quoted in The Telegraph India (2012, 21 November). Everyone Need Not Think the Same: Facebook Girl. *The Telegraph India*. https://www.telegraphindia.com/1121121/jsp/nation/story_16221567.jsp

Shaheen's friend, Rinu Srinivasan, liked, shared and commented on the post on Facebook; she was arrested as well. While the FIR was initially filed under section 295A of the IPC ("deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs"), in addition to section 66A of the IT Act, the former was later replaced by section 505(2) IPC as there was no actual mention of religious belief or religion in either of the girls' comments. Following a large-scale uproar about the girls' arrest, the charges were dropped after about a month.

Years later, the use of India's hate speech sections to stifle political criticism continues. For example, in March 2017, a woman was arrested in Bangalore for Facebook posts she had written which allegedly put Uttar Pradesh Chief Minister Yogi Adityanath in a "poor light." Among the sections she was booked under was section 153A IPC.[62] In April 2017, Prashant Bhushan, a senior advocate and social activist, saw a number of cases slapped on him under section 295A, for a tweet criticising a new policy of the government of Uttar Pradesh, in which he had, among other things, described Lord Krishna as an "eve-teaser".[63]

There are several, intertwined reasons that explain why these sections are frequently used in such an overly broad manner. As mentioned earlier, in free speech jurisprudence in India, a dominant strand accords primacy to public order when free speech and public order seem to clash. In addition, where hate speech in particular is concerned, a close reading of both the hate speech sections in the IPC and of Supreme Court jurisprudence around these sections makes clear that the law gives considerable credibility to the idea that there is an excess of passion and emotion among the Indian people, because of which speech in unregulated or irrational form is believed to be dangerous: as the law states clearly, the feelings of the people need to be tended to. It is therefore that, for example, hate speech jurisprudence in India is deeply concerned not merely with the content of speech but with the form: while speech packaged in a rational form, for example in academic research, may be seen as acceptable, the same message in an artistic format that seeks to offend, shock or disturb might not.[64]

The concurrent existence of these two aspects of Indian hate speech law and jurisprudence has two important consequences. The first is that the question of thresholds disappears into the background when the police receive complaints regarding hate speech. Supreme Court jurisprudence may have developed fairly high standards for the criminalisation of speech under these provisions.[65] For example, in *Ramji Lal Modi v. State of UP*, the Supreme Court, while upholding the constitutionality of section 295A, reconfirmed that the section only penalises insults or attempts at insult of religion or religious feelings that are perpetrated with a deliberate and malicious intent as well as having a tendency to disrupt public order.[66] Similarly, in *Shreya Singhal v. Union of India*, the Court distinguished discussion and advocacy from incitement and noted that only the latter could be limited. But once the feelings of a community are outraged, the question of whether or not the accused did so with deliberate and malicious intent, as required by section 295A IPC, frequently disappears into the background. As the cases of Prashant Bushan and Shaheen Dada mentioned above make clear, to placate the feelings of those outraged, the police come under tremendous pressure to register a case.

Consequently, each time the government gives in to threats of disruption of public order, those who have been outraged find new reason to do so again in the future, as – in a typical case of the heckler's veto – it is the author of the outrageous speech, not those who are threatening disruption, who is silenced. In other words, as Shehla Rashid Shora and Anja Kovacs have pointed out, the hate speech provisions in India's IPC "have allowed reference to a group identity, in combination with the orchestration of an actual or potential threat of group violence, to emerge as effective means for groups to impose their worldview on others."[67] Ironically, those who are most willing to revert to violence become the "custodians" of community identity, while other voices are marginalised.

These challenges are perhaps further heightened because the hate speech sections in the IPC do not take into account the unequal power relations between India's groups, races and religions.

62 Press Trust of India. (2017, 22 March). Bengaluru Woman Faces Police Case For Facebook Posts On Yogi Adityanath. *NDTV*. www.ndtv.com/bangalore-news/bengaluru-woman-booked-for-objectionable-facebook-posts-on-uttar-pradesh-chief-minister-yogi-adityan-1672010

63 Hindustan Times. (2017, 4 April). Prashant Bhushan backs down, admits Krishna tweet was 'inappropriately phrased'. *Hindustan Times*. www.hindustantimes.com/india-news/prashant-bhushan-backs-down-admits-krishna-tweet-was-inappropriately-phrased/story-iRORHk4DSKazaFrB98FkwL.html; Press Trust of India. (2017, 6 April). Fresh case against Prashant Bhushan for his tweet on Lord Krishna. *Deccan Chronicle*. www.deccanchronicle.com/nation/politics/060417/fresh-case-against-prashant-bhushan-for-his-tweet-on-lord-krishna.html

64 Narrain, S. (2016). Op. cit.

65 For an overview, see Law Commission of India. (2017). Op. cit.

66 AIR 1957 SC 620.

67 Shora, S. R., & Kovacs, A. (2013). Op. cit.

While Supreme Court jurisprudence might take into account incitement to discrimination as well as incitement to violence, the text of the law does not distinguish between slander directed at a powerful majority and abuse targeted at a marginalised community or individual.[68]

The only law to fight hate speech in India that does recognise structural and historical discrimination is the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989, which applies to the internet space as well. The Delhi High Court has held that casteist slurs made on Facebook, for example, which target individuals belonging to a scheduled caste or scheduled tribe community, are punishable under this act – even when they are made in a closed group.[69]

Provisions that do not recognise the historical and systemic marginalisation of specific groups of people based on their identity, such as section 153A and 505(2) IPC, are likely to "disproportionately benefit those who already are in a more powerful position than their adversaries, however relative that position might be."[70] As more and more Indians come online, this tension will likely be felt only more acutely.

In addition, the thresholds for the criminalisation of speech included in section 153A and section 505(2) in particular are arguably too low. Former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, has noted that to be criminalised, hate speech should be of a public nature, should at the very minimum present a real and imminent danger, and must contain an obvious intent to harm.[71] Sections 153A and 505(2), however, allow speech to be censored merely because it promotes "disharmony" or "*feelings* of enmity [...] or ill-will" [italics ours]. In fact, in section 505(2), even the mere likelihood of this happening is considered sufficient for prosecution – there is no need to establish intent as well. Where sufficient tension is generated, as in the Shaheen Dada case, this provision, therefore, allows for the criminalisation of what may have been only an innocuous statement – or even a well-intended one – on the grounds that it is "likely" to promote class enmity.

Reform of the law might not always be sufficient. As section 295A comes close to a blasphemy law, it should arguably be scrapped. As Shora and Kovacs have argued:

> While believers of all religious communities, as well as those who do not adhere to any religion, should indeed be protected, religious beliefs as such should not. Without the right to question, be it one's own religion or another, the right to religion becomes meaningless. Those who engage in violence because their own beliefs are questioned or challenged should not be protected by the law on that account.[72]

The constitutional validity of sections 153A, 295A and 298 IPC, among others, is currently being challenged in the Supreme Court by Subramaniam Swamy.[73]

Morality, obscenity and sexual expression

A number of provisions are used to curtail freedom of expression on the internet on the grounds of morality or obscenity. Most prominent among these is section 67 of the IT Act:[74]

> 67. Punishment for publishing or transmitting obscene material in electronic form.—
> Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

The wording of this provision resembles closely that of section 292 of the IPC, which bans the sale, etc. of obscene publications or representations.

68 Ibid.

69 Garg, A. (2017, July 4). Social media slurs on SC/ST punishable: HC. *Times of India*. www.timesofindia.indiatimes.com/india/social-media-slurs-on-sc/st-punishable-hc/articleshow/59432794.cms.

70 Shora, S. R., & Kovacs, A. (2013). Op. cit.

71 La Rue, F. (2012). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/67/357

72 Shora, S. R., & Kovacs, A. (2013). Op. cit.

73 Choudhary, A. (2015, 23 June). Subramanian Swamy challenges hate speech law in SC. *Times of India*. www.timesofindia.indiatimes.com/india/Subramanian-Swamy-challenges-hate-speech-law-in-SC/articleshow/47776651.cms?from=mdr

74 Other provisions that can be and have been used in a similar vein include section 509 IPC (Word, gesture or act intended to insult the modesty of a woman) and provisions of the Indecent Representation of Women (Prohibition) Act, 1986. Their misuse seems, however, less widespread. For reasons of space, we have, therefore, not included a detailed discussion of these provisions in this paper.

In addition, section 294 of the IPC makes obscene songs and dance illegal. Moreover, both section 67 IT Act and section 292 IPC make an exception for material that is "in the interest of science, literature, art or learning or other objects of general concern" or has a "bona fide heritage or religious purpose."

The exceptions listed in the law do not, however, seem sufficient to curtail its misuse. In a groundbreaking study on the use of section 67 of the IT Act in India, Bishakha Datta found that section 67 has been slapped on people in a wide variety of situations, including for speech acts that consist of legitimate political speech.[75]

In some of these cases, the charge of obscenity is completely misplaced, in others overdrawn. For example, in September 2012, Henna Bakshi was booked under section 67, among others, for using abusive language in messages she posted on the Chandigarh traffic police's Facebook page, following an unhappy series of interactions with the police after her car was stolen. While Bakshi did use unparliamentary language in her complaints to the police, only a total of two words used by her in the exchange could be considered to have a sexual connotation.[76] In another example, in November 2016, a Karnataka man was arrested on obscenity charges for allegedly posting on social media a photo of India's prime minister being urinated upon.[77]

A complex mesh of reasons can explain the overuse of such sections. First, as Richa Kaul Padte and Anja Kovacs have noted elsewhere, laws focusing on obscenity and (in)decency in India are based on "the belief that [female] sexuality is an inherently corrupting force that serves to destroy the moral and social fabric of a culture, and therefore, something that needs to be suppressed."[78] Expressions of female sexuality are not only understood as violations of notions of "decency" and "morality" but also as against the broader interests of the state, as sexless, clothed female bodies have come to signify the purity of the nation.[79] Though often defended in the name of women's protection, such laws thus see expressions of female sexuality as a problem, a transgression, and control of women's bodies as essential. Not individual rights but "collective" values that are held dear by dominant groups really are considered the victims here. In other words, through morality, a particular set of power relations is sought to be protected.

Against this backdrop, the ambiguous phrasing of these laws becomes particularly problematic. Scientific or sociologically accepted definitions of what is "lascivious" or "appeals to the prurient interest," what is depraved or corrupting, remain absent. In fact, there is not even agreement on what constitutes "art". As a consequence, in interpreting what qualifies as obscenity, the personal perspectives and values of those making these decisions matter a great deal, and even judges do not always agree with one another when considering these matters. For example, when, in a 1986 case, a High Court judge ruled the description of the female body by a well-known writer obscene, this decision was overruled by the Supreme Court, which believed it to be for the advancement of art.[80] Moreover, Datta's research on the use of section 67 of the IT Act has shown that the situation is even worse on the ground: for many police officers, whose first language is often not English, words such as "prurient" or "lascivious" are simply meaningless.[81]

In addition, it is important to note that obscenity attracts a higher sentence when the offence is an electronic one. Under section 292 IPC, a first conviction only attracts a prison sentence of up to two years or a fine of up to 2,000 rupees, as against three years and 500,000 rupees under section 67 of the IT Act. While a second conviction may attract a term of up to five years under both sections, the IT Act allows for a fine of a whopping one million rupees, as against 5,000 rupees under the IPC. The IPC makes an exception to these relatively milder punishments only when the obscene material is shared with someone younger than 21 years of age.[82]

The fact that the IT Act generally provides for higher sentences for obscenity offences than the IPC has important procedural consequences – and not merely for those convicted. While all the provisions discussed are bailable, the longer sentence

75 Datta, B. (2017). *Guavas and Genitals: An exploratory study on section 67 of the Information Technology Act, India*. Mumbai: Point of View.

76 For a detailed discussion of this case, see Shora, S. R., & Kovacs, A. (2013). Op. cit.

77 The News Minute. (2016, 28 November). Karnataka Man Arrested for Posting Obscene Photo of PM Modi on Facebook. *The News Minute*. http://www.thenewsminute.com/article/karnataka-man-arrested-posting-obscene-photo-pm-modi-facebook-53533

78 Kaul Padte, R., & Kovacs, A. (2013). *Keeping Women Safe? Gender, Online Harassment and Indian Law.* New Delhi: Internet Democracy Project. https://internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/

79 Bose, B. (2006). Introduction. In B. Bose (Ed.), *Gender and Censorship*. New Delhi: Women Unlimited.

80 As noted in Jaising, I. (2006). Obscenity: The Use and Abuse of the Law. In B. Bose (Ed.), *Gender and Censorship*. New Delhi: Women Unlimited.

81 Datta, B. (2017). Op. cit.

82 Section 293 IPC makes illegal the sale, etc. of obscene objects to young persons, prescribing a jail term of up to three years and a fine of 2,000 rupees for a first conviction and of up to seven years and a fine of up to 5,000 rupees for repeat offenders.

under the IT Act makes obscenity under section 67 a cognisable offence, meaning that the police are allowed to start an investigation and make arrests without requiring the permission of a magistrate. In light of the many ambiguities surrounding obscenity laws, and of the widely reported misuse of the section, it deserves to be asked whether the threshold for arrests under the section should not be increased.

Although the Supreme Court's adoption in 2014 of the community standards test over the Hicklin test, in *Aveek Sarkar v. State of West Bengal,*[83] has been widely received as a positive evolution, it does not, so far, seem to have dramatically challenged either the assumptions that underlie the framing of the law or the way it has been applied by police forces across the country.

Established in the English case *Regina v. Hicklin*[84] in 1868, the Hicklin test as formulated by the presiding judge defined the test of obscenity as follows: "whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall."[85] For decades, this test was prominently used in Indian courts of law, most famously to ban *Lady Chatterley's Lover* in India. In *Aveek Sarkar v. State of West Bengal*, the Supreme Court for the first time formulated what it called a "contemporary community standards" test:

> A picture of a nude/seminude woman, as such, cannot per se be called obscene unless it has the tendency to arouse feeling or revealing an overt sexual desire. The picture should be suggestive of deprave mind [sic] and designed to excite sexual passion in persons who are likely to see it, which will depend on the particular posture and the background in which the nude/semi-nude woman is depicted. Only those sex-related materials which have a tendency of "exciting lustful thoughts" can be held to be obscene, but the obscenity has to be judged from the point of view of an average person, by applying contemporary community standards.

As Gautam Bhatia has noted, the judgment was significant for its emphasis on the importance of the background and context in which nude imagery is placed: nudity as such is finally no longer necessarily deemed obscene. Also important is that the Court notes, following the 1957 US Supreme Court case of *Roth v. United States*, that the community standards to be applied should be contemporary: not the standards from India's idealised, mythical golden age, but of today's real-life flesh-and-blood people, should be determining.[86]

Where the judgment remains weak, however, is that it allows for the criminalisation of speech on the grounds of obscenity merely because, following the application of contemporary community standards, an image that contains nudity or semi-nudity is believed to arouse sexual desire or passion. While *Roth v. United States* also required the material to be "patently offensive" and "of no redeeming social value", these additional standards were not referenced in the Indian Supreme Court's ruling.[87] As a consequence, in a country where even mere suggestion is often believed to be inducing passion, much power remains with the eye of the beholder where the right to sexual expression is concerned – as the continuing arrests under this provision make clear.

Perhaps the Court's decision should not be surprising, however. After all, more stringent standards might have run contrary to section 67A of the IT Act, which explicitly criminalises depictions of sexually explicit acts:

> 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.—
> Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

The limitations that apply to section 67 of the IT Act apply here as well, i.e. material that is "in the interest of science, literature, art or learning or other objects of general concern" or has a "bona fide heritage or religious purpose" cannot be criminalised. However, all other depictions of sexually explicit acts are criminalised by section 67A, whether or not

83 (2014) 4 SCC 257.

84 L.R. (1868) 3 Q.B. 360.

85 Quoted in Mazzarella, W. (2011). The Obscenity of Censorship: Rethinking a Middle-class Technology. In A. Baviskar and R. Ray (Eds.), *Elite and Everyman: The Cultural Politics of the Indian Middle Classes*. New Delhi: Routledge.

86 Bhatia, G. (2014, 7 February). Obscenity: The Supreme Court Discards the Hicklin Test. *Indian Constitutional Law and Philosophy*. https://indconlawphil.wordpress.com/2014/02/07/obscenity-the-supreme-court-discards-the-hicklin-test

87 Ibid.

they are "patently offensive" or "of no redeeming social value" and whether or not those involved have consented.

Moreover, where those under 18 years old are concerned, sexual expression is always criminalised in India. Section 67B of the IT Act and sections 13 and 14 of the Protection of Children from Sexual Offences Act, 2012, seek to fight the production, circulation and consumption of child sexual abuse images. Unfortunately, however, the sections in their current wording also criminalise images of a sexual nature that are shared with consent by young people who are in a relationship with each other; none of the provisions provides for an exception in these cases.

Such provisions criminalising all sexual expression further contribute to the portrayal of sexuality as inherently corrupting, while disregarding the importance of consent in any sexual act or in the creation, circulation and publication of images of such acts. In this way, they help to keep existing power relations and their associated conceptions of morality intact. If the writ petition of Kamlesh Vaswani currently under consideration in the Supreme Court is successful, this will only further exacerbate this situation: Vaswani has asked the court not only to ensure that all pornography will be blocked in India, but also that even watching pornography in a private place will be criminalised and will, in fact, be made a non-bailable, cognisable offence.[88] For the moment, while creating, circulating or publishing pornography is illegal, its consumption in private is deemed not to be.

It is notable that section 67A IT Act does not have an equivalent under any other law book in India, meaning that this crime, with its severe sentences, exists only when electronic media are used. Moreover, section 67A IT Act, too, is non-bailable and cognisable, meaning that the barriers to be charged with this crime are few. Perhaps this is what explains why the provision was slapped on a man who had tweeted a 2012 picture of Maharashtra Chief Minister Devendra Fadnavis holidaying on a yacht with his family to suggest that the Chief Minister was squandering taxpayers' money while on an official tour to the United States in 2015.[89] Where sexual expression remains largely taboo, tools to censor it lend themselves easily to misuse indeed.

88 Kamlesh Vaswani v. Union of India & Ors. WP (Civil) 177 of 2013.

89 Bose, A. (2015). A Man Just Got Arrested for Tweeting Chief Minister Devendra Fadnavis' Family Photograph. *Huffington Post*. http://www.huffingtonpost.in/2015/07/11/mumbai-fadnavis-twitter_n_7774592.html

Intellectual property rights

Intellectual property rights are governed under dedicated legislations such as the Indian Copyright Act, 1957, the Trademarks Act, 1999, the Patents Act, 1970, and amendments to these Acts.

Issues of intermediary liability as they relate to intellectual property rights infringement will be addressed in the sub-section on intermediary liability, below. There have also been attempts, on occasion, to use these Acts to directly penalise speech and expression online. We earlier referred to *Tata Sons Limited. v. Greenpeace International & Anr.*,[90] for example, in which the Tata Group sued Greenpeace, an NGO, for defamation and trademark violation when Greenpeace released an online videogame called *Turtles v. TATA* as part of a campaign against Tata's port on beaches in Orissa, as the port was harming olive ridley turtles. The suit was not successful.

A more common concern for free speech on the internet where India's intellectual property rights regime is concerned is the passing of "John Doe" orders by courts. Exercising powers under section 151 of the Civil Procedure Code, courts order the blocking of named and unnamed parties, often for copyright infringement.

For example, as noted earlier, when the producers of Bollywood movies *Lipstick Under My Burkha* and *Jab Harry Met Sejal* approached the Madras High Court in 2017, more than 2,600 websites were blocked as part of an injunction order for copyright infringement. The order required blocking of entire websites, and not just specific URLs that have infringing content.[91]

This is common in the case of "John Doe" or "Ashok Kumar" orders, in which copyright holders (often producers of Bollywood movies or owners of broadcasting rights for large-scale events) approach courts to pass blocking orders, ex parte, against named and unnamed parties who may be publishing copyrighted works of the petitioners.[92] These orders have been found to affect legitimate online businesses and non-infringing websites.[93]

90 CS(OS) 1407/2010.

91 Joshi, D. (2017, 10 August). Madras High Court Issues 'Ashok Kumar' Order to Block the Internet Archive + 2649 Websites. *Spicy IP*. https://www.spicyip.com/2017/08/madras-high-court-issues-ashok-kumar-order-to-block-the-internet-archive-2649-websites.html

92 The principles and procedures evolved and the justification for arraigning unnamed defendants has been argued in a series of posts by the Centre for Internet and Society. See, e.g. Padmanabhan, A. (2014, 30 January). Can Judges Order ISPs to Block Websites for Copyright Infringement? (Part 1). *Centre for Internet and Society*. https://cis-india.org/a2k/blogs/john-doe-orders-isp-blocking-websites-copyright-1

93 Basheer, S. (2016, 24 August). Of Bollywood "Blocks" and John Does: Towards an IP Ombudsman? *Spicy IP*. https://spicyip.com/2016/08/of-bollywood-blocks-and-john-does-towards-a-neutral-ombudsman.html

In the first such case in India, *Tej Television Ltd. v. Rajan Mandal*,[94] a Court Commissioner was appointed to make an inventory of infringing material, equipment used, etc., with the help of technical staff and the police, and to produce a report to be used by the Court. Nowadays, it is common for producers to sub-contract the job of combing through infringing or potentially-infringing websites to external agencies, who tend to err on the site of caution and list more websites for blocking than strictly necessary. As Kian Ganz has noted:

> [U]ntil now, such agencies have had little incentive to get it right. Their bill is usually paid by the copyright holder, who has filed the John Doe order in court and usually doesn't mind if overblocking of websites takes place. And courts realistically do not have enough time to manually check hundreds of file-sharing websites.[95]

Intellectual property rights professor Shamnad Basheer has also noted that it is not practical to require the judges to determine whether the links pertain to specific pages containing the infringing copies:

> [I]s it reasonable of us to expect an overworked and underpaid judge (hit with the pendency pressures and all that) to wade through all 800 links and ascertain infringement for himself/herself? What then is to be done? How are these competing concerns to be balanced out?[96]

The Bombay High Court's Justice Gautam Patel has in the past pointed to the disproportionate nature of blocking and has required a three-step verification before the blocking of URLs, so that the blocking orders are narrowly tailored.[97]

State laws touching on intellectual property rights and their infringement provide an additional challenge where freedom of speech and expression is concerned: going above and beyond what the Indian Copyright Act allows for, they consider copyright infringement as a violation worthy of preventive detention. States like Tamil Nadu, Maharashtra and Karnataka have made amendments to the respective states' preventive detention laws, to make it possible to arrest "audio and video pirates" and "digital offenders".[98]

For example, in August 2014, the Karnataka Prevention of Dangerous Activities of Bootleggers, Drug-Offenders, Gamblers, Goondas, Immoral Traffic Offenders and Slum-Grabbers Act, 1985, was amended to include offences under the Indian Copyright Act, 1957 and the Information Technology Act, 2000. The amendments also brought new categories of "video or audio pirates" and "digital offenders" under the purview of the Act. Section 2(f) of the Act defines "digital offender" as:

> [A]ny person who knowingly or deliberately violates for commercial purposes any copyright law in relation to any book, music, film, software, artistic or scientific work and also includes any person who illegally enters through the identity of another user and illegally uses any computer or digital network for pecuniary gain for himself or for any other person or commits any of the offences specified under section 67, 68, 69, 70, 71, 72, 73, 74 and 75 of the Information Technology Act, 2000.

Further, per Section 2 (vii):

> (vii) In the case of a Video or Audio pirate, when he is engaged or is making preparations for engaging in any of his activities as a Video or Audio pirate habitually for commercial gain, which affect adversely, or are likely to affect adversely, the maintenance of public order.

In the explanation to the section, the meaning of the phrase "video or audio pirate" is further defined:

> (k) "Video or Audio pirate" means a person who commits or attempts to commit or abets the commission of offences of infringement of copy right habitually for commercial gain, in relation to cinematograph film or a record embodying any part of the sound track associated with the film, punishable under the Copy Right [sic] Act, 1957 (Central Act XIV of 1957).

Section 13 of the Act allows the state government to undertake preventive detention of suspects, without the requirement to be produced before a magistrate for up to 90 days (which may extend up to a year). By allowing for preventive detention of

94 [2003] FSR 22.

95 Ganz, K. (2016, 2 August). The messy battle against online piracy. *Livemint*. http://www.livemint.com/Consumer/YtbRN9fv6ZgZCZOexcsWMI/The-messy-battle-against-online-piracy.html

96 Basheer, S. (2016, 27 June). Udta Punjab: Of Courts, Cuts, Copyrights and Conflicted Counsels. *Spicy IP*. https://spicyip.com/2016/06/udta-punjab-linking-courts-cuts-copyrights-and-conflicted-counsels.html

97 Bajaj, R. (2016, 28 July). Bombay HC Effectively Transforms John Does from Swords to Shields – Delineates Most Robust Safeguards to Date. *Spicy IP*. https://spicyip.com/2016/07/bombay-hc-effectively-transforms-john-does-from-swords-to-shields-delineates-most-robust-safeguards-to-date.html

98 Chari, M. (2014, 06 August). Why many states are using the 1923 Goondas Act to curb digital piracy. *Scroll*. http://scroll.in/article/673042/Why-many-states-are-using-the-1923-Goondas-Act-to-curb-digital-piracy

persons suspected of pirating audio or video material for purposes outside of commerce, the Act goes well beyond the scope of liability under the Indian Copyright Act, 1957. Many intellectual property rights and free speech scholars have argued that the provisions are unconstitutional.[99]

Other limitations of freedom of expression

In the previous section, we saw how a variety of grounds are used in India to criminalise speech and expression in ways that are not acceptable. However, free speech is not only curtailed through problematic criminal charges against those who speak; it is also frequently restrained in other objectionable ways. In this section, we will examine five such methods that have had a significant impact on free speech online in India.

Government powers to block content

A first provision of immediate relevance here is section 69A of the IT Act, which provides the central government with the "power to issues directions for blocking for public access of any information through any computer resource," when it is "necessary or expedient to do so, in the interest of sovereignty and integrity of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to the above."

While the IT Act of 2000 also allowed the central government to block content on the grounds of obscenity, this is no longer the case under the amended Act of 2008. Seeing that the likelihood of political abuse of censorship powers is considerably smaller when censorship grounds are narrowly and clearly defined, the removal of obscenity from this provision is a most welcome evolution.

As required by the IT Act, the procedures and safeguards subject to which such blocking may be carried out have been detailed in the Information Technology (Procedures and Safeguards for Blocking Access of Information by Public) Rules, which were notified in October 2009.

Under these Blocking Rules, every ministry or department of the government of India as well as state governments and union territories and any agency of the central government have to appoint a Nodal Officer to which "any person may send their complaint."

If the organisation in question is satisfied that there is indeed reason to take action, it can then forward the complaint, through its Nodal Officer, to the Designated Officer. The Designated Officer is an officer not below the rank of Joint Secretary and may "on receipt of any request from the Nodal Officer of an organisation or a competent court, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored, or hosted in any computer resource" for any of the reasons specified in section 69A of the IT Act and listed above.

However, where the request comes through a Nodal Officer, the Designated Officer can only do so after the request has been examined by a committee "consisting of the Designated Officer as its chairperson and representatives, not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team."

Where possible, the Rules stipulate, the person or intermediary hosting the information will be informed of the inquiry and will get the chance to submit their replies and clarifications; the Rules require the person or intermediary to be given at least 48 hours' notice. In addition, the committee's recommendation to block has to subsequently be approved by the Secretary in the Department of Information Technology under the Ministry of Communications and Information Technology. A Review Committee is supposed to meet at least once every two months to re-examine the legitimacy of all blocking orders.

While the blocking regime under section 69A of the IT Act and its attendant rules is, thus, fairly well circumscribed, requiring a range of approvals and recognising the right to be heard of the owner of the content in question, there are a few aspects of the regime that remain open to improvement.

Allowing content to be blocked simply because it is expedient to do so violates international standards which require that censorship should be necessary and the least restrictive means required to achieve the purported aim. In the absence of these qualifications, the provision has the potential to open the door to censorship that is overly broad.

The inclusion of incitement to the commission of a cognisable offence as a ground for blocking is arguably problematic for the same reason: in established international human rights jurisprudence, incitement is recognised as a ground for censorship specifically when it concerns a clear, demonstrable and immediate incitement to *violence*, or sometimes, discrimination. These qualifications are absent in section 69A and the Blocking Rules.

99 Bhatia, G. (2014, 5 August). Goondagiri Of The Goonda Act. *Outlook India*. www.outlookindia.com/website/story/goondagiri-of-the-goonda-act/291593; Chaudhary, N. (2014, 13 August). Karnataka's 'Goondas Act' – An examination. *Spicy IP*. https://www.spicyip.com/2014/08/guest-post-karnatakas-goondas-act-an-examination.html

Further adding to these concerns is the fact that the last clause of the Blocking Rules explicitly makes transparency in the blocking regime an impossibility. The clause reads: "strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof." In other words, while the phrasing of section 69A of the IT Act and the attendant rules raise a range of concerns regarding their impact on freedom of expression, those same rules also make it impossible for us to assess whether such concerns are indeed justified or whether the purposes for which content is restricted are in fact wholly legitimate.

Moreover, at no point in the process do the section or the rules require the intervention of a judicial body. The crucial role that courts should play, and have played, in democratic societies in decisions that curtail the right to freedom of speech has been disregarded.

While content bans in the offline world have generally been made public in India, it thus becomes almost impossible for the public to challenge online censorship undertaken under this section in court if so desired. The only time at which a challenge becomes possible is when a blocking order is leaked. For example, earlier this year, the government used its powers under this section to ask Twitter to block 115 handles for "propagating objectionable contents." The handles included a range of accounts that allegedly take controversial positions regarding the conflict in Kashmir. The government's request became public knowledge after Twitter, in disregard of the Blocking Rules under section 69A, emailed all account holders involved to inform them that "an official correspondence" was received which claimed that the content of their accounts violates Indian law. When journalists followed up on the incident with Twitter, Twitter linked to a copy of the request that was available on the internet. According to this document, the request for blocking was done in "the interest of public order as well as for preventing any cognisable offence relating to this referred in section 69A of the IT Act."[100]

The constitutional validity of section 69A of the IT Act and the validity of the rules made under that section were challenged in *Shreya Singhal v. Union of India*. The petitioners questioned, among other things, the absence of a guaranteed hearing of the author of the content before a decision is made; the limited procedural safeguards when compared to those provided in the case of offline bans (under section 95 and 96 of the Criminal Code of Procedure); and the confidentiality provision. However, the court rejected the petitioners' arguments, on the grounds that the provision is narrowly framed and that a number of procedural safeguards are foreseen, even if those are different from safeguards for offline content. The constitutionality of both the provision and rules was upheld.

Intermediary liability

The Indian authorities do not always draw on section 69A to block content. Figures reported by Google in its Transparency Report indicate that the company receives a substantial number of takedown requests from Indian government officials. In 2016, the Indian government made 575 such requests, asking for 5,370 pieces of content to be taken down.[101] Only 52 of those requests, relating to 196 items, were made by the judiciary. The rest came from the executive branch of government. Google complied in 14% of cases. Requests such as those reported by Google in its transparency reports are frequently made under section 79 of the IT Act and its attendant rules, the Intermediary Guidelines Rules 2011, both of which concern intermediary liability and safe harbour.

Intermediary liability in the IT Act

The IT Act defines an intermediary as:

> [A]ny person who on behalf of another person receives, stores or transmits that record or provides any service with regard to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

The current version of section 79 was included in the IT Act in 2008; following a number of controversies, section 79 was reframed at that time to more clearly define and circumscribe the circumstances under which intermediaries could become liable. According to the section in its current form, intermediaries are not liable for content they provide access to, provided they do not initiate or select the receiver of the transmission; do not select or modify the information contained in the transmission; and do delete content "expeditiously when receiving actual knowledge or when being notified by the appropriate government or its agency." When this

100 Saha, A. (2017, 4 September). Citing official complaint, Twitter tells Kashmiri handles they are breaking laws. *Hindustan Times*. http://www.hindustantimes.com/india-news/twitter-tells-kashmiri-handles-they-are-breaking-indian-laws-points-to-official-complaint/story-u33dt3gtkKvUjZtpId13fJ.html

101 Google Transparency Report: Government requests to remove content. https://www.transparencyreport.google.com/government-removals/by-country/IN

amendment to the IT Act was first approved, this phrasing was considered a substantial improvement over the earlier version of this section in the IT Act of 2000, and was as such welcomed.

But the additional guidelines that the central government prescribed in April 2011, as it is authorised to do under section 79 of the Act, undid much of the protection and clarity the section was intended to provide. Known as the Intermediary Guidelines Rules 2011, these made it obligatory for intermediaries to inform their users, by means of their terms of service, not to host, display, upload, modify, publish, transmit, update or share a broad range of types of content. In addition to content prohibited by article 19(2) of India's Constitution, this included content deemed "grossly harmful", "harassing", "blasphemous", "hateful", "racially, ethnically objectionable", "disparaging" or that "impersonate[d] another person" or "harm[ed] minors in any way." As many of the grounds for censorship included in the latter group go beyond the grounds of reasonable restrictions established by India's Constitution and are not defined under any other Indian statute, intermediaries were left without any guidelines to judge content. Moreover, under the Intermediary Guidelines Rules, anyone could file a complaint with the intermediary, who then had to act within 36 hours. The intermediary did not have to inform the party who posted the content, and the Intermediary Guidelines Rules did not provide for an automatic right to respond for the aggrieved party, nor for an appeals mechanism.

The privatisation of censorship that the Indian intermediary liability regime thus put into place had the potential to have a deeply chilling effect on free speech in the country. In informal conversations, representatives of several major intermediaries indicated over several years that the number of takedown requests by both government and private parties had grown substantially since the Rules were notified. Moreover, at least in some cases these requests were accompanied by significant political pressure that might have affected intermediaries' decisions. For example, on 5 December 2011, *The New York Times* reported that the then Minister of Communications and Information Technology, Kapil Sibal, had, over a stretch of several months, had a string of meetings with some of the major intermediaries in which he had tried to convince them to manually pre-screen content and remove any objectionable material.[102] Content that Sibal showed to the intermediaries is said to have included both religiously sensitive material that he believed could potentially cause riots and political speech that he deemed unacceptable – including a Facebook page that maligned the president of the Congress Party, Sonia Gandhi.

In the same year, a study conducted by Rishabh Dara, then Google Policy Fellow at the Centre for Internet and Society, clearly brought out that intermediaries tend to err on the side of caution when faced with government requests to take down content.[103] Dara sent rather frivolous takedown notices to seven major intermediaries. Six of them complied, with some even taking down *more* content than Dara had requested. Strictly speaking, affected parties could have gone to the courts in response. Yet as the notice-and-takedown system that was put into place under section 79 lacked transparency, they in many cases might not even have become aware that their rights had been violated.

In *Shreya Singhal v. Union of India,* concerns about the potential for misuse of these provisions, and the weakening of the protections for freedom of expression that they therefore entail, were brought to the Supreme Court. The privatisation of censorship that the Intermediary Guidelines Rules and its parent section entailed, as well as the lack of safeguards in the Rules, were all called into question by the petitioners. In addition, the petitioners argued that the grounds on which both the rules and parent section allowed for censorship were vague and over-broad and went well beyond the subjects specified under Article 19(2) of the Indian Constitution.

The Supreme Court was receptive to the petitioners' arguments, and while stopping short of striking down the section and rules, it read down both. From here onwards, intermediaries have been only obliged to take down content upon receiving "a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to article 19(2) are going to be committed." In such cases, intermediaries are expected to remove content expeditiously. Where the content in question does not fall within the reasonable restrictions mentioned in Article 19(2) of the Constitution and/or where an intermediary has not received a court order or a notification from a relevant government agency, it is not obliged to act.

While the Supreme Court's judgement may have strengthened the legal certainty for both

102 Timmons, H. (2011, 5 December). India Asks Google, Facebook to Screen User Content. *The New York Times*. www.india.blogs.nytimes.com/2011/12/05/india-asks-google-facebook-others-to-screen-user-content

103 Dara, R. (2012, 27 April). Intermediary Liability in India: Chilling Effects on Free Expression on the Internet. *Centre for Internet and Society*. https://www.cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet

intermediaries and authors of content, it is not clear to what extent it has reduced takedowns. Google, for example, received the highest number of requests for the highest number of items ever in 2016; its compliance rate was only marginally higher than that in 2014, before the judgement in *Shreya Singhal v. Union of India* was pronounced.[104] In the case of Facebook, however, a drastic reduction can be observed: in 2016, the year that Facebook started to implement the judgement, it took down 2,753 pieces of content, compared to more than 30,000 the year before, and more than 10,000 in 2014. Facebook takes down content mostly under India's laws protecting religious beliefs and the sentiments of communities, as well as the protection of national symbols.[105]

Whether or not government-requested takedowns have decreased, it deserves to be pointed out that big tech companies in India, such as Amazon, reportedly also resort to tremendous amounts of self-censorship. "Nobody wants bad PR or government ire in an important market over a little nudity or a dead cow," as Pranav Dixit has reported.[106]

Intermediaries and copyright

While section 79 of the IT Act might govern intermediary liability in general, additional provisions for intermediary liability are included in the Copyright (Amendment) Act, 2012. For those who seek to quickly remove material that they disagree with from the internet, this amended version of the Indian Copyright Act, 1957, might in many cases provide an all-too-easy route through which to do so.

At the heart of the regime around intermediary liability and copyright that has emerged in India is the case of *Super Cassettes Industries Ltd. v. Myspace Inc.*[107] In this case, the former sought to hold social network MySpace liable for copyright infringement. In his judgment, Justice Singh referred to section 81 of the IT (Amendment) Act, 2008, to argue that the safe harbour provisions in the IT Act did not apply in this case. Section 81 of the IT Act states that "nothing in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957." With this, Justice Singh pointed out a crucial lacuna in the law.

The gap was partially resolved in 2012 when several amendments to the Copyright Act of 1957 were passed in Parliament. Two of these entail a limited safe harbour provision, and thus have direct import for internet intermediaries.

The first amendment, section 52(1)(b) in the new Act of 2012, absolves intermediaries from liability for copyright infringement where the storage of infringing content is "transient or incidental" and part of a purely technical process of transmission or communication.

The second amendment, section 51(1)(c) in the amended Act, does the same when the transient or incidental storage of content is "for the purpose of providing electronic links, access or integration," on the condition that doing so "has not been expressly prohibited by the rights holder" and "unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy."

The amendment further states that "if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work" claiming copyright infringement, the former is obliged to disable access to the content in question for a period of 21 days, or until receiving a court order. "In case no such order is perceived before the expiry of such period of 21 days, [the person responsible for the storage of the copy] may continue to provide the facility of such access."

As Sunil Abraham has pointed out,[108] the amendment clearly privileges the concerns of intellectual property rights-holders, as the intermediary is obliged under the law to remove the content in question even before the validity of the complaint has been proved. Because of this, the mechanism provided for under the amended Copyright Act is likely to have a chilling effect on free speech. Moreover, the likelihood of ISPs automatically and voluntarily reinstating content once the legal waiting period of three weeks has passed and no court order has been received, is low.

Abraham's colleague Pranesh Prakash goes even a step further. If the complaint turns out to be false – either because the complainant is not the rights-holder or because the content does not entail a violation of the rights-holder's copyright – there

104 Google Transparency Report: Government requests to remove content. https://www.transparencyreport.google.com/government-removals/by-country/IN

105 Facebook (2016). Government requests report. https://www.govtrequests.facebook.com/country/India/2016-H2/

106 Dixit, P. (2017, 12 July). American Tech Companies Are So Afraid Of Offending Indians That They're Censoring All Their Products. *Buzzfeed News*. https://www.buzzfeed.com/pranavdixit/why-silicon-valley-is-censoring-itself-as-it-expands-in?utm_term=.ry6qKDEboD#.jcApR71bJ7

107 Super Cassettes Industries Ltd. v. Myspace Inc. 2011 (48) PTC 49 (Del).

108 Abraham, S. (2012, 10 June). Copyright amendment: bad, but could have been much worse. *Smart Investor*. www.smartinvestor.business-standard.com/market/Compnews-120087-Compnewsdet-Sunil_Abraham_Copyright_amendment_bad_but_could_have_been_much_worse.htm#.WaZ9h98xDec

is no punishment for the person who filed the complaint. Given this lack of punishment, Prakash has argued, the law is open to widespread abuse: it allows anyone "to remove content from the internet without following any 'due process' or 'fair procedure'."[109]

Clearly, this amendment to the Copyright Act therefore violates the principles of necessity and proportionality that are integral to the validity of any action that seeks to censor content online.

But there are two further aspects of the judgment that were remarkable and also deserve attention here. First, when determining whether MySpace had knowledge of the presence of copyright-infringing content on its platform, Justice Singh highlighted the mechanisms instituted by MySpace to trail and curtail copyright infringement, as well as efforts by MySpace to cooperate with industry in this area, as one indication that MySpace did indeed have such knowledge (the Justice was not convinced they also authorised such actions though). With this, the Justice went against the grain of what is increasingly considered best practice in this area in the international community, where such proactive measures on the part of intermediaries generally have been lauded. Justice Singh's pronouncements on this issue were of importance because having actual knowledge was a ground on which intermediaries can lose the safe harbour provided to them by section 79 IT Act as well.

Finally, the Justice also argued that "if the defendants are put to notice about the rights of the plaintiff in certain works, the defendants should do preliminary check in all the cinematograph works relating Indian titles before communicating the works to the public rather than falling back on post infringement measures." He further stated:

> if there is any due diligence which has to be exercised in the event of absence of any provision under the Act, the said due diligence must be present at the time of infringement and not when the infringement has already occurred so that the infringement can be prevented at the threshold and not when the same has already occurred.

Various aspects of MySpace working practices convinced the Justice that it should be technically feasible to do so. Although Justice Singh made his pronouncements in a case relating to copyright, with this, he was the first to put the supposed need for a pre-screening mechanism on the table.

Fortunately, in December 2016, following an interlocutory appeal, a two-judge bench of the Delhi High Court overturned the 2012 order, and ruled that pre-screening requirements cast an enormous burden on intermediaries.[110] This welcome order cited the challenges that inhere in requiring intermediaries to regulate speech on the internet.

Ongoing challenges to India's intermediary liability regime

Challenges to India's intermediary liability regime, nevertheless, continue. Two separate, ongoing cases in the Supreme Court are of particular importance.

In *Sabu Mathew George v. Union of India & Ors.*,[111] the petitioner seeks to ensure that advertisements for services related to sex selective abortions do not show up in search engine results – be they paid results or organic results – as they violate section 22 of India's Pre-Conception and Pre-Natal Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994 (henceforth PCPNDT Act). Section 22 reads:

> 22. Prohibition of advertisement relating to pre-conception and pre-natal determination of sex and punishment for contravention.—
> (1) No person, organisation, Genetic Counselling Centre, Genetic Laboratory or Genetic Clinic, including Clinic, Laboratory or Centre having ultrasound machine or imaging machine or scanner or any other technology capable of undertaking determination of sex of foetus or sex selection shall issue, publish, distribute, communicate or cause to be issued, published, distributed or communicated any advertisement, in any form, including internet, regarding facilities of pre-natal determination of sex or sex selection before conception available at such Centre, Laboratory, Clinic or at any other place.
> (2) No person or organisation including Genetic Counselling Centre, Genetic Laboratory or Genetic Clinic shall issue, publish, distribute, communicate or cause to be issued, published, distributed or communicated any advertisement in any manner regarding pre-natal determination or pre-conception selection of sex by any means whatsoever, scientific or otherwise.

109 Prakash, P. (2012, 23 May). Analysis of the Copyright (Amendment) Bill 2012. *Centre for Internet and Society*. www.cis-india.org/a2k/blog/analysis-copyright-amendment-bill-2012

110 Nair, B. (2016, 25 December). Breaking News: Del HC Division Bench Rules in Favour of Safe Harbour for Intermediaries in MySpace-T Series Copyright Dispute. *Spicy IP*. https://www.spicyip.com/2016/12/breaking-news-division-bench-rules-in-favour-of-safe-harbour-for-intermediaries-in-myspace-t-series-dispute.html

111 WP (Civil) 341 of 2008.

(3) Any person who contravenes the provisions of sub-section (1) or sub-section (2) shall be punishable with imprisonment for a term which may extend to three years and with fine which may extend to ten thousand rupees.

Explanation.—For the purposes of this section, "advertisement" includes any notice, circular, label, wrapper or any other document including advertisement through internet or any other media in electronic or print form and also includes any visible representation made by means of any hoarding, wall-painting, signal, light, sound, smoke or gas.

In response, the Court directed Google, Yahoo! and Microsoft, in September 2016, to block results for a number of keywords and keyword strings provided by the Court. In April 2017, the Court clarified that only results that violate section 22 PCPNDT Act should be blocked. It noted:

> It is made clear that there is no need on the part of anyone to infer that it creates any kind of curtailment in his right to access information, knowledge and wisdom and his freedom of expression. What is stayed is only with regard to violation of Section 22 of the Act.[112]

However, it remains unclear how intermediaries can ensure that only illegitimate content will be blocked if content is blocked based on keywords and keyword strings. This is even more so as it is not clear how the word "advertisement" is to be interpreted by the intermediaries in this case: while the intermediaries are arguing for a narrow definition, the Solicitor-General has argued for a broad understanding, in which case the distinction between legitimate and illegitimate content becomes even more difficult to discern and a much wider range of content may be affected. The debate on what constitutes an "advertisement" in this case is still ongoing in court.

In addition, in September 2016, the court ordered the three intermediaries to develop an "auto-block" mechanism: an in-house procedure or method to ensure that advertisements or searches that are introduced into the system but are violating the PCPNDT Act will not be shown in the results even when they are not included in the results for the keyword searches mentioned above. The intermediaries protested this interim order, arguing that it runs counter to section 79 of the IT Act and the Court's judgement in *Shreya Singal v. Union of India*.

Rather than rescinding its interim order, however, the Court further ordered the intermediaries, in February 2017, to appoint an "In-House Expert Body", which will be responsible for ensuring that any words or keywords that are in violation of the PCPNDT Act will be deleted immediately. Where the Expert Body has any doubt, it can seek guidance from the Nodal Agency appointed by the Union of India on directions of the Court. The Nodal Agency will also intimate the intermediaries of any violating content that has been brought to its notice by the public. For the moment, the burden on intermediaries to proactively prevent violating content from appearing online remains.

A second case in which intermediaries have been requested to prevent content from being uploaded is *In Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendation*.[113] The case concerns a request to the Supreme Court by NGO Prajwala to stop the circulation of videos depicting child sexual abuse, rape and gang rape. The report of a court-ordered Expert Committee to make recommendations on how to address this problem was put on record on 6 July 2017 and all recommendations on which there was consensus were subsequently adopted by the Court on 23 October 2017.

This included a recommendation that content-hosting platforms, search engines and the government work together "in formulating [a] process for proactively verifying, identifying and initiating take down" of all such content. Though it was recognised that effective implementation of this recommendation requires further research, the Court also noted that in developing such mechanisms to enable real-time filtering at the time content is uploaded, techniques based on artificial intelligence, deep learning and machine learning should be used.

The Court's interim order contains no indication of what kind of safeguards will be used to prevent censorship that is overly broad when implementing these mechanisms, nor is there an explicit recognition that such safeguards are important. Seeing that, as explained earlier, legitimate sexual expression is controversial in India as well, this is cause for concern. Unless clear safeguards are put in place, this case, while laudable in its aims, might inadvertently end up undermining the progressive intermediary liability regime that *Shreya Singhal v. Union of India* had put into place.

112 WP (Civil) 341 of 2008, order dated 13 April 2017. http://supremecourtofindia.nic.in/pdf/cir/2017-04-13_1492086489.pdf

113 SMW (Crl.) 3 of 2015.

Social media group administrators and intermediary liability

If the big intermediaries might have benefited from the greater legal clarity around India's intermediary liability regime to some extent, the pressure may simply have shifted to a different set of actors: the authorities' alleged concern for public order has led them to expect special vigilance on the part of WhatsApp group administrators.

With more than 200 million users, India is WhatsApp's biggest market, and it one of the most popular forms of digital communication in the country. It is also considered a prime means to spread fake news and disinformation.[114] For example, when a Muslim man was murdered in Bisara village near Dadri, in September 2015, on suspicion of storing beef in his fridge, this was followed by an apparently planned rumour-mongering campaign on WhatsApp and Twitter.[115] In another case that same year, in Solapur, Maharashtra, rumours about thefts, looting and possible child kidnapping that circulated in WhatsApp groups led to widespread fears.[116]

The authorities have attempted to contain the spread of such rumours by putting the burden of vigilance on group administrators, even though such administrators arguably are intermediaries. In 2016, two state governments issued directives holding WhatsApp group administrators liable for any message circulated in the group. In Jammu and Kashmir, the circular issued by the District Magistrate of Kupwara additionally required new WhatsApp groups to be registered with the district social media centre by the administrator. In Jharkhand, the circular released by government officials in Dumka held that social media group administrators would be held liable wherever they did not remove group members who had shared incorrect, misleading or seditious information or did not report such an incident to the authorities in cases where this information could affect peace in society.[117]

In April 2017, an order issued jointly by the District Magistrate and Senior Superintendent of Police in Varanasi, Prime Minister Modi's constituency, noted that where fake information or rumours or statements that could cause religious disharmony were circulated in a social media group, such messages needed to be refuted by the group administrator and the poster of the message would need to be removed from the group. In addition, the order also required all such posts to be reported to the nearest police station. "In the event of inaction from the group admin, he or she will be considered guilty and action will be taken against the group admin," the order said.[118]

Some relief seemed to arrive when in December 2016, in *Ashish Bhalla v. Suresh Chawdhury & Ors,*[119] the Delhi High Court noted that it could not see how a WhatsApp group administrator could be held liable for allegedly defamatory messages that were circulated in the group about one of the group's members – especially since messages do not require the administrator's approval before being posted. However, as these remarks were merely made by the Court in its rejection of a complaint on the grounds of non-disclosure of cause of action, the judgment cannot be considered a conclusive judicial determination on the matter of liability of social media group administrators in India.

And indeed, arrests of WhatsApp group administrators have continued since then. For example, in Karnataka, in May 2017, the administrator of a WhatsApp group on which "ugly and obscene" images of the prime minister were circulated, was arrested.[120] And in July 2017, two WhatsApp group administrators were arrested in Chennai because objectionable images of the state finance minister and a female actress were posted in their group by a member.[121]

Network shutdowns

The number of internet shutdowns in India has been steadily increasing over the past five years. While the Software Freedom Law Centre, which has been

114 Singh, M. (2017, 24 February). WhatsApp hits 200 million active users in India. *Mashable India*. www.mashable.com/2017/02/24/whatsapp-india-200-million-active-users/#F569eCmwisqG

115 The Hindu. (2016, 6 October). Dadri lynching: Police identify rumour-mongers. *The Hindu*. www.thehindu.com/news/national/other-states/dadri-lynching-police-identify-main-accused/article7727750.ece

116 Anima, P. (2015, 28 August). The new tattler in town. *The Hindu Business Line*. www.thehindubusinessline.com/blink/know/the-new-tattler-in-town/article7587041.ece

117 Dan, S. (2016, 28 December). Are WhatsApp Group Administrators Liable For Members' Statements? *The Wire*. https://www.thewire.in/89903/whatsapp-group-administrators-liability

118 Press Trust of India. (2017, 21 April). WhatsApp admins beware: Offensive posts can land you in jail. *Hindustan Times*. www.hindustantimes.com/tech/whatsapp-admins-beware-offensive-posts-can-land-you-in-jail/story-iddtcX54taNah803ZIlwxJ.html

119 CS (OS) No. 188/2016.

120 Deccan Chronicle. (2017, 3 May). WhatsApp group admin in Karnataka arrested for sharing offensive posts on PM. *Deccan Chronicle*. www.deccanchronicle.com/technology/in-other-news/030517/whatsapp-group-admin-in-karnataka-arrested-for-sharing-offensive-posts-on-pm.html; ANI. (2017, 3 May). Beware! Here's why a WhatsApp group admin was arrested. *DNA India*. www.dnaindia.com/india/report-k-taka-whatsapp-admin-arrested-for-offensive-posts-on-pm-modi-2425854

121 Thirumurthy, P. (2017, 27 July). WhatsApp group admins and member arrested for posting obscene images of TN Minister. *The News Minute*. www.thenewsminute.com/article/whatsapp-group-admins-and-member-arrested-posting-obscene-images-tn-minister-65848

tracking internet shutdowns in the country, found reports of three such crackdowns in 2012, by late August the number for 2017 was already 47.[122] In addition, the Indian government has had no qualms about blocking SMS and/or voice in various parts of Kashmir and the North-Eastern states of India at different points in time, even before internet shutdowns became a regular occurrence, as well as restricting SMS across the country on several occasions.

The internet is shut down in India for a wide range of, sometimes trivial, reasons. For example, between February 2016 and March 2017, an ongoing agitation by the Jat community for reservations led to mobile internet services being suspended eight times in parts of Haryana, in addition to one complete block of internet services. In February 2016, mobile internet services were also suspended across Gujarat for four hours to prevent cheating in the Revenue Accountants Recruitment Exam. In March 2015, all internet services were stopped for 48 hours in Nagaland after a video of the lynching of an accused rapist went viral. In August 2016, mobile internet services were disrupted for two days in parts of Arunachal following the death of the state's former Chief Minister, Kalikho Pul. And in June 2017, mobile internet services, and later also broadband services, were stopped for at least a week, following violent clashes between the Gorkha Janmukti Morcha (GJM) and security forces after the GJM called for a complete strike in its agitation for a separate Gorkhaland. With 49 shutdowns since 2012, the state that has seen the greatest number of internet suspensions in India is Jammu and Kashmir. Many of these shutdowns are precautionary and seek to prevent the spreading of information or rumours.[123]

As section 69A of the IT Act, discussed above, allows the government to block content on a number of grounds, it could be argued that this section also provides the Indian authorities with the legal ability to switch off, under particular circumstances, access to all or parts of the internet in India. Rule 9 of the Blocking Rules that accompany section 69A explicitly allows for the Secretary of the Department of Information Technology to order intermediaries to block access "in any case of emergency nature, for which no delay is acceptable" without giving such intermediaries an opportunity of hearing. Within 48 hours, this order has to be brought for consideration and approval to a larger committee, which includes representatives of the Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team. However, the rules do not specify within which time period the committee has to provide a recommendation with regard to the order, nor for that matter do the Rules or the IT (Amendment) Act specify anywhere under which conditions a situation can be considered an "emergency" in the first place.

In practice, however, internet shutdowns in India have happened under section 144 of the Criminal Code of Procedure, which reads:

> 144. Power to issue order in urgent cases of nuisance of apprehended danger.—
> (1) In cases where, in the opinion of a District Magistrate, a Sub- divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, there is sufficient ground for proceeding under this section and immediate prevention or speedy remedy is desirable, such Magistrate may, by a written order stating the material facts of the case and served in the manner provided by section 134, direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management, if such Magistrate considers that such direction is likely to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, of an affray.
> (2) An order under this section may, in cases of emergency or in cases where the circumstances do not admit of the serving in due time of a notice upon the person against whom the order is directed, be passed ex parte.
> (3) An order under this section may be directed to a particular individual, or to persons residing in a particular place or area, or to the public generally when frequenting or visiting a particular place or area.

This provision has been used to shut down the internet in various states, including on the order of police commissioners, who can exercise the powers of executive magistrates in emergencies. Any order issued under this section can be in force for no more than two months from the time of its making, unless it is extended by the state government for a further six months.

These powers were first used in 2004 by the Mumbai police, to block the website hinduunity.org; anti-Islamic material accessible on this website was thought to be potentially inflammatory. In the following years, the Mumbai and Pune police in particular have used their power to block internet content on

122 SFLC.in. Internet Shutdowns Tracker. www.internetshutdowns.in
123 Ibid.

several occasions.[124] The content in question generally related to Shivaji, the Marathi warrior-hero, or to political figures, including Bal Thackeray and B. R. Ambedkar. In one such instance, an Orkut community containing supposedly "objectionable and derogatory" comments about Shivaji was blocked; at the time of blocking, the one-month old community had a mere 101 members.[125]

In recent years, however, section 144 has been used more and more often to shut down the internet altogether, especially in times of social or political controversy or tension. This use of the section, earlier called on predominantly to restrict the right to assembly offline where such assembly could lead to a potentially volatile situation, massively expanded the censorship capacities of the authorities, providing them with a blunt instrument to silence people that they could wield like a sledgehammer. Further adding fuel to the worry is the state government's ability to extend such orders by an additional six months, without the intervention of a court or other independent body. Such provisions open the door to political misuse.

Despite these concerns, in February 2016, the Supreme Court dismissed a plea challenging the power of state governments to shut down internet services using section 144. The plea argued that only section 69A of the IT Act should be used to shut down the internet; section 69A provides only the central government with the powers to block. The Supreme Court dismissed the plea on the ground that internet shutdowns at times are necessary to maintain law and order. A Gujarat High Court order had earlier upheld a ban on mobile internet services imposed by the Gujarat government in August 2015 on the same grounds. The unsuccessful plea in the Supreme Court had sought to challenge that order.

Irrespective of the Court's verdict, network shutdowns in India have drawn international attention. In May 2017, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, and UN Special Rapporteur on the situation of human rights defenders, Michel Forst, called upon India to restore internet and social media networks in Jammu and Kashmir in particular. In April 2017, the state government had blocked 22 social media sites/apps, including Facebook, WhatsApp, YouTube and Skype. "The internet and telecommunications bans have the character of collective punishment," stressed Kaye, "and fail to meet the standards required under international human rights law to limit freedom of expression."[126]

The ban on social networking sites, which was issued under section 5(2) of the Indian Telegraph Act, 1885, was challenged before the Srinagar High Court for being arbitrary, ineffective and amounting to excessive delegation as it focuses on the medium rather than on the content of messages.[127] Section 5(2) reads as follows:

> On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

Though the High Court refused to stay the ban, it noted that such a ban could only ever be temporary and required periodic review.[128] The state government lifted the ban after a month; it allegedly had not been very successful, as users used virtual private networks (VPNs) to circumvent the

124 OpenNet Initiative. (2012). *India*. www.opennet.net/research/profiles/india

125 Press Trust of India. (2006, 18 November). Orkut forum blocked over Shivaji comments. *DNA India*. http://www.dnaindia.com/india/report-orkut-forum-blocked-over-shivaji-comments-1064711

126 Office of the United Nations High Commissioner for Human Rights. (2017, 11 May). India must restore internet and social media networks in Jammu and Kashmir, say UN rights experts. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21604&LangID=E

127 Parray, M. A. (2017, 9 May). Social media ban challenged; HC declines stay. *Kashmir Reader*. www.kashmirreader.com/2017/05/09/social-media-ban-challenged-hc-declines-stay; Peerzada, A. (2017, 10 May). Plea challenges social media ban in J&K. *The Hindu*. www.thehindu.com/todays-paper/tp-national/plea-challenges-social-media-ban-in-jk/article18417526.ece

128 Tantry, I. (2017, 17 May). Social media ban likely to continue in Kashmir. *The Tribune*. www.tribuneindia.com/news/jammu-kashmir/social-media-ban-likely-to-continue-in-kashmir/408099.html

restrictions[129] even though the government reportedly had tried to block VPNs as well.[130]

On 7 August 2017, the Government of India released, quietly and without any preceding public consultation, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017. The rules have been framed under section 7 of the Indian Telegraph Act, 1885, which reads:

> 7. Power to make rules for the conduct of telegraphs.—
> 1) The Central Government may, from time to time, by notification in the Official Gazette, make rules consistent with this Act for the conduct of all or any telegraphs established, maintained or worked by the Government or by persons licensed under this Act.
> (2) Rules under this section may provide for all or any of the following among other matters, that is to say: [...]
> (b) the precautions to be taken for preventing the improper interception or disclosure of messages; [...]
> (k) any other matter for which provision is necessary for the proper and efficient conduct of all or any telegraphs under this Act.

Rule 2(1) of the new rules reads:

> Directions to suspend the telecom services shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India or by the Secretary to the State Government in-charge of the Home Department in the case of a State Government (hereinafter referred to as the competent authority), and in unavoidable circumstances, where obtaining of prior direction is not feasible, such order may be issued by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorised by the Union Home Secretary or the State Home Secretary, as the case may be:
> Provided that the order for suspension of telecom services, issued by the officer authorised by the Union Home Secretary or the State Home Secretary, shall be subject to the confirmation from the competent authority within 24 hours of issuing such order:
>
> Provided further that the order of suspension of telecom services shall cease to exist in case of failure of receipt of confirmation from the competent authority within the said period of 24 hours.

Any directions for suspension of services in addition need to be reviewed within five days by a Review Committee set up by the union or state government.

Insofar as the rules provide a clearer procedure for network shutdowns and limit the authorities that can impose them, taking this power away from district-level authorities, they seem a step forward. However, seeing that both the authority who can order a shutdown and the Committee that reviews that order are from within the executive, there remains cause for concern. As the rules do not specify what can be considered a "public emergency" or a "threat to public safety", broad concerns around public order and public safety will likely continue to trump concerns for freedom of expression and other human rights, at enormous cost to the latter. As they can rarely be considered a solution that is necessary and proportionate, internet shutdowns should only be resorted to in the most extreme of circumstances. It is unlikely, however, that these rules will ensure that shutdowns will indeed become such an exception. Rather, they seem to legitimise the practice, even if they may perhaps help to somewhat reduce the number of shutdowns in the future. Moreover, while the rules regulate "temporary" shutdowns, they do not provide any restrictions on the time period for which an order for suspension can be valid. In addition, while the reasons for an order of suspension of services need to be recorded in the order, the rules do not make it mandatory for the government to make those reasons public.

ISPs are committed to follow government orders to shut down services as per their licence agreements. For example, the Unified Licence Agreement states explicitly that the government has:

> the right to take over the service, equipment and networks of the Licensee (either in part or in whole of the service area) in case any directions are issued in the public interest by the Government of India in the event of a National emergency/war or low intensity conflict or any other eventuality.

Conflicts such as those in Kashmir and the North-East are of the low intensity variety. In addition, ISP licence agreements note explicitly that the government reserves the right to keep any area out of the operation zone of the service if implications of security so require.

129 Hindustan Times. (2017, 27 May). J-K government lifts ban on social media in Kashmir. *Hindustan Times*. www.hindustantimes.com/india-news/j-k-government-lifts-ban-on-social-media-in-kashmir/story-U9dfX6tswZhmrqTYFITk5J.html

130 Kashmir Post. (2017, 4 May). Cyber Cell begins snapping VPN's: Blocking the blocked. *Kashmir Post*. www.kashmirpost.org/2017/05/04/cyber-cell-begins-snapping-vpns-blocking-the-blocked

Concerns related to net neutrality

The terms of access to media and communications infrastructure are a crucial element in the exercise of freedom of speech and expression. However, fundamental rights are applicable against the state, but media and communications infrastructure is often privately owned. To what extent, then, can the state justify infrastructure regulation?

Matters of infrastructure regulation were agitated under the protection of freedoms under Article 19 of the Constitution as far back as 1962, in the case of *Sakal Papers (P) Ltd. & Oth. v. Union of India.*[131] In this case, the editor of a newspaper and its readers challenged the validity of the Newspaper (Price and Page) Act, 1956, which empowered the central government to fix prices of newspapers according to the number of pages and allocation of space for advertising. One of the questions before the court was whether the regulation of prices of newspapers by the government was an infringement on the right to freedom of speech and expression of the press. The court ruled that the legislation affected the right to freedom of the press, which forms part of Article 19(1)(a). Regulation of advertising space, and its indirect impact on circulation, was found to be an infringement on the right to freedom of speech and expression.

In the context of the internet, the Telecom Regulatory Authority of India (TRAI) consultation on discriminatory pricing of data services brought in sharp focus the question of whether or not, and to what extent, to regulate service offerings of telecom service providers in the larger public interest.

This consultation happened against the background of the emergence of "zero-rated" internet plans in India – such as telecom operator Bharti Airtel Ltd.'s Zero plan and Facebook's Internet.org-turned-Free Basics. Network operators on their own, or in partnership with internet companies, were offering data plans which would provide selective access to the internet for a lower price or for free. One of the issues before the authority was: what principles should guide the decision to regulate such plans (or to abstain from regulating)? Or in other words, what are the first principles towards which any policy on differential pricing should be aimed?

TRAI noted that the consultation was initiated because two key principles of tariff regulation were being affected: non-discrimination and transparency.[132] Many additional considerations were forwarded in the comments made by stakeholders, including innovation, competition, non-discriminatory access to users and, crucially in the context of this report, the right to freedom of speech and expression. The consultation paper acknowledged this:

> Several responses have drawn a critical link between the internet and its role in preserving the constitutional guarantees of right to free speech and expression under Article 19(1)(a) of the Constitution. As observed by the Supreme Court, in the S*ecretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal*, (1995) 2 SCC 161, para 201 (3)(b) allowing citizens the benefit of plurality of views and a range of opinions on all public issues is an essential component of the right to free speech. This includes the right to express oneself as well as the right to receive information as observed by the Supreme Court in the *Indian Express Newspapers (Bombay) Put. Ltd. v. Union of India*, (1985) 1 SCC 641 (para 68) case. Both of these components viz., right to express oneself as well as the right to receive information are critical elements in the use of the internet. The Authority is of the view that use of internet should be in such a manner that it advances the free speech rights of the citizens, by ensuring plurality and diversity of views, opinions, and ideas.[133]

Arguments in favour of zero-rating included that there was no stopping a customer to avail of the full internet by paying for data; that platforms (at least in the case of Free Basics) would be open to any app, content or service; that such regulating is paternalistic; and that disallowing zero-rating would kill business models and affect the freedom of these companies to conduct trade, etc.

Following several rounds of public consultations, TRAI passed a regulation in February 2016 that prohibited discriminatory pricing of data services on the basis of content.[134]

Given the value that the public internet has provided for economic, social, political and cultural ends, allowing a selection of applications, content and services to be accessed for a negligible amount or for free would likely have led to the exclusion of a large section of the population from being able to make use of the medium to the fullest. It would also have undone the relatively "permission-less" nature of innovation by applications developers and content and service providers on the internet,

131 1962 AIR 305.

132 Telecom Regulatory Authority of India. (2016, 08 February). Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 (2 of 2016). www.trai.gov.in/sites/default/files/Regulation_Data_Service.pdf. Para 2 of Explanatory Memorandum.

133 Ibid. Para 24.3 of Explanatory Memorandum.

134 Ibid.

including where these are regular citizens or not-for-profits rather than commercial entities, arguably affecting their freedom of speech and expression.

Without going as far as to provide a definitive list of characteristics which justify regulation of private commercial entities, the explanatory memorandum to the TRAI regulation notes that changes to business models and commercial arrangements should pay heed to the unique architecture of the internet, including its "end-to-end design principle", according to which features specific to an application reside in the communicating end nodes, rather than in the intermediary nodes of the network. This principle is central to net neutrality.

The internet has become the most active public square, where political speech is discussed, and public opinion mobilised. The state has a role to play in ensuring that such a space is not unduly controlled by gatekeepers. As private players mediate access to a public good, the internet, they have an obligation to ensure that there is no discrimination on the grounds of who the service is being offered to. As observed in several submissions to the above-mentioned consultation, the Supreme Court has previously held that when private parties discharge what amounts to a public function, they must be held to a public law standard.[135]

Consultations on a broader framework for net neutrality, with similar potential ramifications for the right to freedom of expression online, have also been held by TRAI since then, as well as by the Department of Telecommunications. The outcome of these consultations is awaited.

Surveillance

It has been established by courts[136] as well as by research[137] that mass surveillance has a chilling effect on speech and expression. In India, such concerns have arisen especially in the context of mass surveillance programmes. Some of these, such as the Central Monitoring System (CMS) and National Intelligence Grid (NATGRID), have been designed for the specific purpose of mass communications surveillance; others, such as the Unique Identity Project (Aadhaar) and the seeding of Aadhaar numbers in other databases, have tremendous potential for mass surveillance but were not developed explicitly for this purpose.

The CMS has been operationalised through a mere executive order. In addition, the licence terms of Unified Access Services (UAS) Licensees and Unified Service Licensees were amended in 2013 to require the setting up of interception store and forward (ISF) servers and integration with the Lawful Interception Systems at the licensee's premises.[138] These servers were to be connected to Regional Monitoring Centres, which are in turn connected to the CMS. The CMS infrastructure, operated by Telecom Enforcement Resource and Monitoring (TERM) cells, enables interception of all communications over the networks in a systematic way such that authorities do not have to interface with the nodal officers of telecom service providers for interception requests.

As per section 4 of the Telegraph Act, all ISPs and telecom companies require a licence from the central government to do business. While licences contain a number of clauses requiring ISPs to safeguard the privacy and confidentiality of the information of their customers, they also require ISPs to maintain extensive logs of user activity, which need to be available in real time to the telecom authority, and to cooperate with government agencies when required to do so. In practice, however, ISPs only kept a log of customers' internet protocol addresses, as well as selectively monitoring specific users' activity at the government's request.[139] With the establishment of the CMS, the government now no longer needs to rely on telecom companies' cooperation.

NATGRID is an initiative of the Ministry of Home Affairs. According to the Ministry's website, NATGRID "has been conceived to develop a cutting edge framework to enhance India's counter-terror capabilities." The project, started in 2011, seeks to connect 21 databases held by different agencies of the government like the Customs Department, Income Tax Department, etc., through agreements. The Central Board of Direct Taxes issued a notification earlier this year to share "bulk information" including Permanent Account Numbers (PAN), taxpayers' names and demographic and biometric details like photographs and thumbprints with NATGRID.[140] Such all-round access by intelligence agencies to

135 Unnikrishnan v. State of Andhra Pradesh, 1993 SCC (1) 645.

136 Shreya Singhal v. Union of India, AIR 2015 SC 1523.

137 Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal, 31*(1). https://www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

138 Ministry of Telecommunications and Information Technology. (2013, 11 October). Amendment 2 of 13. www.dot.gov.in/sites/default/files/DOC231013.pdf?download=1

139 Philip, J. T. (2010, 30 December). Intelligence bureau wants ISPs to log all customer details. *Economic Times*. https://economictimes.indiatimes.com/tech/internet/intelligence-bureau-wants-isps-to-log-all-customer-details/articleshow/7187899.cms?intenttarget=no

140 Central Board of Direct Taxes, Department of Revenue, Ministry of Finance. (2017, 21 June). Notification 54 of 2017. www.incometaxindia.gov.in/communications/notification/notification54_2017.pdf; Press Trust of India. (2017, 22 June). NATGRID to get PAN, taxpayer data access. *Economic Times*. www.economictimes.indiatimes.com/news/economy/policy/natgrid-to-get-pan-taxpayer-data-access/articleshow/59270998.cms

citizens' data exists without external accountability mechanisms or independent oversight.

News reports indicate that several ministries[141] and police departments[142] have also begun or plan to start operations to monitor social media. Such programmes are likely to have a chilling effect on speech on the internet as well, and the question of reasonability arises when these are ongoing programmes, seeking to gauge the "public's moods".

As legal scholar Gautam Bhatia has noted, if surveillance is an issue that affects freedom of speech and expression, then it needs to have statutory backing according to Article 19 of the Constitution, and such a law should pass the test of reasonability. He observes that the determination of whether programmes like the CMS are reasonable restrictions in the interests of "security of the state" and "public order" would depend upon what line of precedent the court would take:

> Under the Ramji Lal Modi line of cases, with their broad understanding of the phrase "in the interests of", the surveillance regime will be easy to justify (it is hardly deniable that it bears some relation to public order and security). If, on the other hand, the narrower test of Lohia is followed, then the burden upon the government will be much greater.[143]

Indeed, even though government officials maintain that the requirements under section 5(2) of the Indian Telegraph Act, 1885, read with Rule 419A will continue to apply at least in the case of the CMS, the development of these mass surveillance programmes through executive orders seems to be the apex of a continuous hollowing out of checks and balances in India's surveillance regime that protect freedom of speech and expression as well as privacy.[144]

Two acts are central to this regime: the Indian Telegraph (Amendment) Act 2006, which governs telecom service providers (including ISPs), and the IT (Amendment) Act 2008, which has wider application. Both Acts penalise the unlawful interception of communications (e.g. sections 24 and 25 of the Telegraph Act; sections 43 and 66 of the IT Act). They also permit interception by the state under specific conditions.

Section 5(2) of the Indian Telegraph (Amendment) Act 2006 allows for such interception "on the occurrence of any public emergency, or in the interest of the public safety," provided that "it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence."

The Indian Telegraph Rules 2007 specify, in rule 419A, that in normal circumstances, such interception can only be ordered by officers of the rank of Secretary, either in the Ministry of Home Affairs, where the central government is concerned, or in the Home Department, where a state government is concerned. Moreover, such an order can only be issued "when it is not possible to acquire the information by any other reasonable means" and has to contain reasons. The rule further includes a range of safeguards to be observed during interception, as well as imposing limits on periods of both data collection and retention.

Most of the provisions made under the Indian Telegraph Act and its attendant rules have been retained in the IT Act. However, there is one significant difference: section 69 of the IT (Amendment) Act 2008 has done away with the requirement for "a public emergency" or "the interest of the public safety", while adding "the defence of India" and "for investigation of any offence" to the list of grounds on which surveillance is allowed.

As Prashant Iyengar has pointed out, the requirement of "a public emergency" or a clear threat to "public safety" as preconditions had earlier put a clear damper on the Indian government's ability to legally intercept communications.[145] In *PUCL v. Union of India*, referring to the Indian Telegraph Act, the Court had observed:

> [E]ven if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or in public order or for preventing incitement to the commission of

141 Press Trust of India. (2017, 23 June). Government plans a new social media policy to check anti-India activities. *Economic Times*. www.tech.economictimes.indiatimes.com/news/internet/government-plans-a-new-social-media-policy-to-check-anti-india-activities/59276445; Hindustan Times. (2016, 24 February). Govt to monitor social media 24x7 to counter negative comments, blogs. *Hindustan Times*. www.hindustantimes.com/india/govt-to-monitor-social-media-24x7-to-counter-negative-comments-blogs/story-6Phot5wXXtMbzTYTKpm9kI.html

142 Puri, N. (2013, 9 March). India sets up social media monitoring lab. *ZDNet*. www.zdnet.com/article/india-sets-up-social-media-monitoring-lab

143 Bhatia, G. (2016). *Offend, Shock, or Disturb*. New Delhi: Oxford University Press.

144 Xynou, M. (2017, 30 January). India's Central Monitoring System (CMS): Something to Worry About? Centre for Internet and Society. https://www.cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

145 Iyengar, P. (2011). *Privacy in India - Country Report - October 2011*. Bangalore: Centre for Internet and Society. https://ssrn.com/abstract=2302978

> an offence, it cannot intercept the message, or resort to telephone tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires.[146]

This important constraint has been done away with in the case of digital communications.

At the same, by allowing for interception of communications in the course of the investigation of any offence, the range of communications that have the potential to legally come under the state's radar has increased exponentially. While interception in the case of an economic offence, for example, generally would not have been possible under the Indian Telegraph Act, it is very much so under the new IT Act.

The considerable expansion of the state's powers to intercept communications within its borders is particularly worrying in the light of reports that even telephone tapping, regulated by the far more stringent Telegraph Act, is widespread. For example, in February 2011, telecom service provider Reliance Communications told the Supreme Court that it had tapped, on order of the authorities, 151,000 phone numbers between 2006 and 2010. This amounts to 30,000 telephone interceptions every year – or 82 every day – by a single service provider.[147] As safeguards such as the Review Committee, which has to meet at least once every two months to assess the legality of all orders, are unlikely to work effectively under such circumstances, this has raised serious questions about the extent to which the law is being followed, in letter or in spirit.

Legislative amendments have been proposed to the Telegraph Rules for the insertion of Rule 419B, which would give legislative authority to conduct mass interception of communications. As per Access Now's report to the UN Special Rapporteur on freedom of speech and expression:

> Besides the deployment of the infrastructure and operations for the CMS programme, the Union Government also proposed amendments to the legal environment on interception in India, in the form of a proposed Rule 419B to the Telegraph Rules. This would have provided legal cover for the CMS programme and real time surveillance operations on Indian licensed network operators. Proposed in 2013, this amendment to the Telegraph Rules has not yet been advanced.[148]

While the Indian Telegraph Act regulates only interception, section 69 of the IT Act applies to monitoring and decryption as well.

Since its inception, the Aadhaar project has raised concerns for its potential for mass and pervasive surveillance. Only in 2016, the government enacted legislation to govern the different aspects of the project: the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. With subsequent notifications by the government requiring the Aadhaar number of individuals to be linked to everything from government benefits to mobile numbers and bank accounts, it has created an unprecedented infrastructure with huge surveillance potential.

Section 33 provides for the disclosure of this information, including identity information and authentication records, when it is required in the interest of "national security" in pursuance of a direction of an officer who is Joint Secretary to the Government of India or a higher rank, on behalf of the central government. Every such direction is to be reviewed by an Oversight Committee. Such orders will be valid for a period of three months from the date of issue, and may be extended for three more months after the Oversight Committee reviews it.

Further, the purpose of use of the information and the terms of sharing, publication and display of the information are not fixed, and may be specified through regulations.[149] This means that the scope of use of the information held by the Unique Identification Authority of India can be expanded at the executive's will, without the Act having any further checks and balances.

Future violations through draft laws

In March 2017, the Law Commission of India submitted Report No. 267 on Hate Speech to the central government, in pursuance of a request to do so by the Supreme Court in March 2017.[150] This report suggests

146 PUCL v. Union of India. AIR 1997 SC 568.

147 Mahapatra, D. (2011, 15 February). Over 1 lakh phones are tapped every year. *Times of India*. www.articles.timesofindia.indiatimes.com/2011-02-15/india/28545822_1_lakh-phones-subscriber-base-provider

148 Access Now. (2016). Access Now submission to the UN Special Rapporteur on the protection of the right to freedom of opinion and expression study on Telecommunications and Internet Access Sector. www.ohchr.org/Documents/Issues/Expression/Telecommunications/AccessPart_II.docx

149 Section 23(2)(k) of the Act allows the Unique Identification Authority of India (UIDAI) to share information about individuals in such manner as may be specified by regulations. Section 29(2) permits the sharing of identity information other than core biometric information, in such manner as may be specified by regulations. Section 29(4) permits the publication and display of an individual's core biometric information or Aadhaar number for purposes as may be specified by regulations.

150 Law Commission of India. (2017). Op. cit.

amendments to the Indian Penal Code by the insertion of Sections 153C and 505A, expanding the scope of hate speech laws in India, including by explicitly recognising hate based on sex, gender identity, sexual orientation or disability, among others.

In October 2017, the Internet Freedom Foundation released a leaked copy of another report: the recommendations of an expert committee headed by TK Visvanathan, which was formed after section 66A of the IT Act was struck down as unconstitutional.[151] This report proposes further changes to both draft provisions proposed in the Law Commission report on hate speech, including to make explicit that these sections apply to communications on the internet as well. While these changes overall are improvements over the proposals by the Law Commission, its proposed new section 505A of the IPC, in particular – and contrary to what the report claims – continues to suffer from the same issues of vagueness and overbreadth that afflicted section 66A of the IT Act.

For example, many of the terms used to describe communication that would be criminalised under the section are imprecise and nebulous. Similarly, although the proposed section specifies that there needs to be an "intention to cause fear of injury" or an "intention to cause alarm", this qualification arguably does not pass the "clear and present danger" test. In *Shreya Singhal v. Union of India*, the Supreme Court had ruled that discussion or even advocacy of a cause was not sufficient to justify any restriction on the right to freedom of speech and expression; only when this reaches the level of incitement does Article 19(2) apply.

A number of other laws and policies that are currently in the drafting stage have the potential to negatively impact the right to freedom of speech and expression on the internet in the future as well.

The Draft Prohibition of Indecent Representation of Women and Children Bill, 2012,[152] sought to widen the scope of its parent act to include communications made over electronic media. The bill proposed new definitions for "indecent representation of women", "electronic form" and "publish". This bill released by the Ministry of Women and Child Development is still pending.

The Ministry of Home Affairs released the Draft Geospatial Information Regulation Bill[153] in 2016, and called for comments from all stakeholders. The bill sought to regulate the acquisition, publication, modification and dissemination of any representation of spatial attributes of India. After business interests and user groups across the country sent comments against the proposed bill, there have been no developments. This bill would have affected several internet-age businesses involved in logistics management, humanitarian relief efforts and, of course, users, and would limit freedom of speech by limiting their use of maps.

The Draft National Encryption Policy 2015[154] released by the Department of Electronics and Information Technology sought to increase the security of the internet and related information systems by regulating the strength of encryption that may be used. However, the policy if implemented would have imposed great burdens on users and businesses to store in plaintext any information exchanged via electronic media for up to 90 days after the communication was made. Contrary to the stated objectives, such a policy would have been disastrous to the security of communications and information networks, and to user privacy.

At present, although this does not seem to be enforced, telecom licences disallow ISPs from using bulk encryption, as well as prescribing a maximum 40-bit encryption for individuals, groups or organisations without obtaining permission from the government. For stronger encryption, prior permission from the government is required and the decryption key, split into two parts, is to be deposited with the government.

Following the unanimous verdict by the nine judges of the Supreme Court in *KS Puttaswamy v. Union of India*,[155] we can expect legislation on data protection in the near future. The judgment also affirms that the right to privacy, which is enshrined in the right to life, affects the enjoyment of the right to freedom of speech and expression under Article 19(1)(a).

Summary and conclusions

While the Shreya Singhal judgement might have signified an important victory for freedom of expression in the digital space in India, many challenges remain. Criminal defamation is used all too often by powerful actors to silence critical voices. Laws regarding sedition and the protection of national symbols are misused to curtail political dissent. Provisions regarding hate speech often reward those who respond with threats of violence to

151 TK Visvanathan Committee. (n/d). *Recommendations of TK Visvanathan Committee*. New Delhi: TK Visvanathan Committee. https://internetfreedom.in/files/documents/recommendations.of.t.k.visanathan.committee.pdf

152 www.prsindia.org/billtrack/the-indecent-representation-of-women-prohibition-amendment-bill-2012-2576/

153 www.prsindia.org/uploads/media/draft/Draft%20Geospatial%20Bill,%202016.pdf

154 www.netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf

155 KS Puttaswamy v. Union of India. WP (CIVIL) 494 of 2012.

speech they do not agree with, rather than ensuring a safe space to speak for all. Expressions of sexuality are frequently penalised irrespective of consent or intent; women's agency rarely seems to matter here. Even copyright laws are applied in ways that disregard freedom of expression and criticism of court decisions is all too easily seen as contempt.

Even where there is no threat of arrest, freedom of expression is frequently hampered through overly broad government blocks, limited protections of intermediaries and sledgehammer methods such as network shutdowns. In addition, concerns around network neutrality and surveillance can further silence many voices, including, in the latter case, through self-censorship.

As the country has such a solid reputation as a democracy, this long list of challenges to freedom of expression that can be found in India may come as a surprise. A central tension that runs throughout almost all of these challenges, however, is that between public order and freedom of expression – a tension that was debated as early as during the time of India's Constituent Assembly. It is because many lawmakers as well as government officials continue to believe that public order trumps freedom of expression wherever the two clash that restrictions can be imposed in India with relative ease – and the judiciary provides only limited relief. Only when the courts, too, start to see a need to carve out space for freedom of expression even when public order is in disorder, will stronger protections of the right to freedom of expression likely emerge. Especially in the age of the internet, hecklers should not be allowed to veto speech, if the potential of the internet to allow a voice to even the most marginalised in the country is really to bloom.