Xindex
the voice of free expression

India: Digital freedom under threat?

November 2013

India: Digital freedom under threat?

Policy Paper, November 2013

Author: Melody Patry
Editor(s): Mike Harris, Kirsty Hughes

With thanks to Brian Pellot, Marek Marczynski, Pam Cowburn, Alice Kirkland.

Photo credits: cover, page 10, and 17, Purushottam Thakur; page 4, Shutterstock.

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this liscence, visit http://creativecommons.org/licenses/by-nc-sa/3.0/

About Index

Index on Censorship is an international organisation that promotes and defends the right to freedom of expression.

Index uses a unique combination of journalism, campaigning and advocacy to defend freedom of expression for those facing censorship and repression, including journalists, writers, social media users, bloggers, artists, politicians, scientists, academics, activists and citizens.

Contents

Introduction

The rules India makes for its online users are highly significant – for not only will they apply to 1 in 6 people on earth in the near future as more Indians go online, but as the country emerges as a global power they will shape future debates over freedom of expression online.

India is the world's largest democracy and protects free speech in its laws and constitution.[1] Yet, freedom of expression in the online sphere is increasingly being restricted in India for a number of reasons– including defamation, the maintenance of national security and communal harmony, which are chilling the free flow of information and ideas. Many of the most restrictive laws and technical means used to enforce these restrictions are recent developments that have undermined India's record on freedom of expression. A mix of social and political pressure, alongside the terrorist attacks in Mumbai in 2008, has led to this decline, but civil society is beginning to push back.

This paper explores the main digital issues and challenges affecting freedom of expression in India today and offers some recommendations to improve digital freedom in the country.

Constraints on digital freedom have caused much controversy and debate in India, and some of the biggest web host companies, such as Google, Yahoo and Facebook, have faced court cases and criminal charges for failing to remove what is deemed "objectionable" content. The main threat to free expression online in India stems from specific laws: most notorious among them the 2000 Information Technology Act (IT Act) and its post-Mumbai attack amendments in 2008 that introduced new regulations around offence and national security.

New regulations introduced in 2011 oblige internet service providers to take down content within 36 hours of a complaint, whether made by an individual, organisation or government body, or face prosecution. This is problematic in many ways: it makes intermediaries liable for content which they did not author on websites and platforms which they may not control and encourages them to monitor and pre-emptively censor online content, which leads to the excessive censorship of content.

Meanwhile, the arrest and prosecution of citizens who have posted content deemed "grossly harmful", "harassing", or "blasphemous" has multiplied. Censorship through the criminalisation of online speech and social media usage is troubling, especially when it affects legitimate political comment or harmless content.

Other issues addressed in this paper include how individual states and the national government of India restricts online communications using filters, and increasingly engages in mass surveillance, which can chill freedom of expression. One of the most pressing challenges to digital freedom remains India's use of network shutdowns in certain regions, it is claimed, in order to prevent public disorder. Ensuring access to the digital world remains a national challenge. With only 10 percent of the Indian population online today, there may be a billion new Indian netizens online in the future. How India enables this to happen will be a major challenge. While India is an increasingly influential player in global internet governance, now is a critical time to analyse its domestic regulations and policies that

1 Article 19 of the Indian Constitution protects freedom of speech and expression. Government of India, 'The Constitution of India,' as modified up to the 1st December 2007, Article 19. (1)(a) 'All citizens shall have the right to freedom of speech and expression' http://lawmin.nic.in/ accessed on 23 September 2013.

will shape the path not only for the people of India but also for regional neighbours and emerging democratic powers.

This paper is divided into the following chapters: online censorship; the criminalisation of online speech and social media; surveillance, privacy and government's access to individuals' online data; access to digital; and India's role in global internet debates.
The online censorship chapter looks at intermediary liability and the issue of state and corporate censorship mainly via takedown requests and filtering and blocking policies. The criminalisation of online speech chapter covers the prosecution of Indian citizens who post content on the net, including on social media.

The surveillance chapter looks at the recent revelations on the extraordinary extent of domestic surveillance online, and how it contributes to chilling free speech online. It also looks at privacy and government's access to individuals' online data. The access chapter covers obstacles and opportunities in expanding digital access across the country.

Finally, the chapter on India's role in global internet debates looks at India's positioning in the current debates that will result in potentially significant changes to net governance in the next two years.

This policy paper is based on research from London and a series of interviews conducted between June and October 2013 with a range of interviewees from civil society, internet businesses, political figures and journalists.

Recommendations

To end internet censorship and provide a safe space for digital freedom, Indian authorities must:

- Stop prosecuting citizens who express legitimate opinions in online debates, posts and discussions;
- Revise takedown procedures, so that demands for online content to be removed do not apply to legitimate expression of opinions or content in the public interest, so not to undermine freedom of expression;
- Reform IT Act provisions 66A and 79 and takedown procedures so that content authors are notified and offered the opportunity to appeal takedown requests before censorship occurs;
- Stop issuing takedown requests without court orders, an increasingly common procedure;
- Lift restrictions on access to and functioning of cybercafés;
- Take better account of the right to privacy and end unwarranted digital intrusions and interference with citizens' online communications;
- Maintain their support for a multistakeholder approach to global internet governance.

1 Online Censorship

Since 2003, the institutional structure of internet censorship and filtering has centred on the Indian Computer Emergency Response Team (ICERT), a department of the Ministry of Communication and Information Technology that serves as a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to specific websites.[2] This chapter will outline how takedown requests, both with and without court orders, are commonplace, and demonstrate that corporations sometimes contribute to censorship by over-complying with government requests. Along with filtering and blocking policies, these procedures are inconsistent and often threaten freedom of expression in India. With so many methods being used to restrict online speech, there is lively debate in India around how censorship affects fundamental freedoms and society.

"There is no definition of what 'obscenity' and 'incitement' constitutes. Because of the vagueness of the law on the one hand, and the obligations of the law on the other hand [taking down offensive content], the door is opened to interpretation and subjectiveness," says Rajeev Chandrasekhar, a member of the upper house of the Indian Parliament.[3] The vagueness of the law has led to people being arrested and charged for innocuous posts and tweets. The Information Technology Act (IT Act) and its 2008 amendments do not provide a clear legal definition of what is offensive and there is no common view in society of what can or cannot be said online and offline, leading to uncertainty. This has resulted in a growing tendency to report content deemed "offensive" and demand its removal.

Intermediaries - web companies that host content but do not produce it – tend to over-comply with takedown notices out of fear of being liable for offensive content and then prosecuted. The over-compliance of internet intermediaries with takedown notices is concerning as it removes from the internet content which is entirely legitimate.

Compounding this problem is the lack of an appeal process. Intermediaries in India are neither required to notify people when their posts or photos are censored nor give them an opportunity to appeal the decision. In practice, this situation creates an indirect form of censorship when not the government but intermediaries become censors.

Takedown Requests

Takedown requests, when properly regulated, implemented and subjected to judicial oversight, can be an effective way for copyright owners and aggrieved individuals to remove illegal content from the web. When takedown procedures are inconsistent or inadequately defined, as is the case in India, such requests can, and often do, chill freedom of expression.

In the 2008 amendments to the IT Act, the government acted to limit intermediary liability and standardise notice and takedown procedures under Section 79 of the IT Act. This marked a positive move to curtail the worst abuses of the law and protect intermediaries. The question of intermediary liability is particularly complex in India due to vague laws around defamation and public order. The Indian authorities have tended to prioritise control or regulation of free speech to "protect communal harmony". The protection of communal harmony was cited as a major factor behind the move in 2011 by the Indian Central Government to issue the Information Technology [Intermediaries Guidelines] Rules – also called the 2011 IT Rules – requiring intermediaries to remove infringing content within 36 hours if someone reports it as offensive.

2 Freedom House, 'Freedom on the Net 2012: India', http://www.freedomhouse.org/report/freedom-net/2012/india accessed on 9 September 2013.
3 Index on Censorship interview, 30 August 2013.

Many medium and small internet businesses have been vocal in criticising the impact of these rules, a piece of secondary legislation linked to the IT Act.[4] They denounce the onerous conditions they face as intermediaries in the event of prosecution. The confusion around intermediary liability laws encourages privatisation of censorship and causes a great deal of uncertainty for businesses which they argue hinders innovation.[5]

In 2011, the Bangalore-based Centre for Internet and Society (CIS) ran a series of tests to see how intermediaries responded to bogus takedown request within the 36-hour timeframe. Six of seven intermediaries over-complied with requests, meaning they restricted more content than legally required. Hundreds of pages were taken down at the expense of legitimate expressions.[6] This over-compliance demonstrates a real chilling effect on freedom of expression, as many intermediaries are overwhelmed with requests or do not have the legal expertise to properly handle them in a manner that protects freedom of expression.

In April 2013, the Government issued a Clarification on the Information Technology [Intermediaries Guidelines] Rules, under Section 79 of the IT Act. The clarification addresses the controversial 36-hour period and says that the intermediaries shall respond or acknowledge to the complainant within 36 hours of receiving the complaint/grievances, and then initiate appropriate action in line with the law rather than actually take down the content. While this clarification is helpful, the law remains flawed and still subjects intermediaries to criminal prosecution for failure to comply in a short period of time. This narrow timeframe, which does not specifically take into account public holidays or weekends, puts intermediaries in a difficult position where they are required to be overly zealous in taking down content that may be entirely legitimate.

Government requests for the removal of illegal or offensive content is steadily on the rise around the world, but this is especially the case in India. A benchmark to track this trend is the Google Transparency Report, where India leads in the number of takedown requests issued without court orders. Indian authorities cite national security concerns to justify many of their takedown requests without court orders.[7] For example, in the second half of 2012 the Indian Computer Emergency Response Team cited public order and ethnic offence laws to issue a request for "The Innocence of Muslims" video clips to be taken down. The video clips had sparked disturbances in India's north-east regions and Google locally restricted the "Innocence of Muslims" video clips from YouTube and several other YouTube videos and comments.

While "The Innocence of Muslims" case launched a debate over how religious or cultural sensibilities balance with free expression, the lack of judicial oversight in content takedown and political interference are common practice in India.[8] The removal of "The Innocence of Muslims" demonstrated how the politics of fear is intruding into the online environment.[9]

---

4 Government of India, Ministry of Communications and Information Technology, "The Information Technology (Electronic Service Delivery) Rules, 2011", http://deity.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf accessed on 19 November 2013.

5 The Economist Intelligence Unit, 'Good to grow? The environment for Asia's Internet business' (9 July 2013), http://asiainternetcoalition.org/advdoc/2c083eb6cd1ae38cee3826e1ad6a2a6e.pdf accessed on 10 September 2013.

6 Centre for Internet and Society, 'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011', http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf accessed on 4 September 2013.

7 Indian authorities requested, without court orders, that 2,529 items be removed between July and December 2012 – a 90 percent increase over the first half of the year 2012. Google, 'Google Transparency Report', http://www.google.com/transparencyreport/removals/government/IN/ accessed on 5 September 2013.

8 Kenan Malik and Nada Shalout, Index on Censorship, 'Should religious or cultural sensibilities ever limit free expression?,' http://www.indexoncensorship.org/2013/08/should-religious-or-cultural-sensibilities-ever-limit-free-expression/ accessed on 25 September 2013.

9 Rebecca MacKinnon and Ethan Zuckerman, Index on Censorship, 'Don't feed the troll,' http://www.indexoncensorship.org/2012/12/dont-feed-the-trolls-muslims/ accessed on 25 September 2013.

Google is not the only company dealing with a significant number of takedown requests. For small start-ups and internet service providers, a large number of takedown requests can encourage those afraid of penalties to over-comply, removing URLs that do not link to illegal content. A consequence of the IT Act and of the over-compliance would be the delegation of essential executive function to private parties like Google, Facebook or MouthShut.com to censor and restrict free speech of citizens or else face legal challenges over user content.

Case study: "MouthShut.com"

On 29 April 2013, MouthShut.com, India's leading online consumer review website, filed a petition in the Supreme Court of India to nullify the 2011 IT Rules. The petition pleads that the 2011 IT Rules be declared illegal, null and void as they are ultra vires of the Constitution. [1]

Faisal Farooqui, founder of MouthShut.com, has said that the company has "been threatened with hundreds of legal notices, cybercrime complaints and defamation cases. At other times, officers from various police stations call our office, demanding deletion of various reviews or face dire consequences under the IT rules".[2]

Under the IT rules, MouthShut is required to remove content within 36 hours of receiving a request (a request does not necessary need to be issued by a court order but can be filed by any individual). The problem is that MouthShut.com receive requests under IT Rules "to remove any negative review about a company or brand simply because they don't like it, irrespective of the facts stated in the review."

"It is submitted that the impugned Rules impose significant burden on it forcing it to screen content and exercise online censorship, which in turn impacts the freedom of speech and expression of its customers, thereby risking a loss of its large consumer base or incurring legal costs and facing criminal action for third party user-generated content," Farooqui said.

1 Times of India, 'Supreme Court to Examine validity of Information Technology rules' (30 April 2013), http://articles.timesofindia.indiatimes.com/2013-04-30/internet/38929437_1_intermediaries-guidelines-accuracy-censorship accessed on 30 August 2013.
2 Medianama, News and Analysis of Digital Media in India, 'MouthShut Challenges the IT Rules In The Supreme Court Of India', (29 April 2013), http://www.medianama.com/2013/04/223-mouthshut-it-rules-supreme-court-of-india/ accessed on 25 September 2013.

Filtering and Blocking

India engages in the widespread blocking and filtering of websites. The Indian Computer and Emergency Response Team is able to make executive orders to internet service providers to block websites. The range of sites that are censored is quite broad and ranges from human rights and freedom of expression content to extremism and porn.[10] This section addresses the problematic role that a government authority, the Indian Computer and Emergency Response Team (ICERT), has in being able to order internet service providers to selectively filter content, including without court instruction.

10 Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, OpenNet Initiative, 'Access Contested. Security, Identity, and Resistance in Asian Cyberspace' (September 2011), http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf accessed on 10 September 2013.

Despite an announcement to install filtering mechanisms at India's international gateways, government attempts at filtering have not been entirely effective because blocked content has quickly migrated to other websites and users have found ways to circumvent filtering.[11] However, India's filtering and blocking policies remain problematic both because of the scale of the compliance with ICERT but also the scope of its powers. Many have argued that giving ICERT filtering power through executive order violates constitutional jurisprudence, especially since the blocking mechanism created under the IT Act provides for no direct review or appeal procedures and is a permanent block.[12]

Beyond excessive powers to filter, India's government also holds significant and disproportionate powers to block content. Merely in order to gain a government licence to operate, internet service providers (ISPs) in India must agree to block sites and individual users when national security needs arise and to prevent the transmission of "obscene" or "objectionable" material. Since 2008, these powers have been extended to block more than just content that is "obscene". The newly added Section 69A of the IT Act also grants power to the central government, "in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order," to issue directions to block public access to any information from any "computer resource." This executive power is significant and should be subjected to justice oversight to avoid misuse of the law by the executive.

Only a limited number of specified individuals or institutions can make official complaints and recommendations for investigation to ICERT. These include high-ranking government officials, the police, government agencies and "any others as may be specified by the Government". In return, ISPs have to comply with blocking orders from ICERT. Since 2006, blocking requests can also come from individuals reporting content they personally consider to be offensive or obscene. Individuals can do this by filling a Public Interest Litigation petition in order to put pressure on the government or justice authorities to issue a filtering notice.

This is having a significant impact on freedom of expression. Tests undertaken of the blocking practices of ISPs revealed variations, suggesting that ISPs go beyond direct blocking orders to pro-actively block content. This practice results from licensing agreement that require ISPs to bock internet sites as identified by the Telecom Authority but also to prevent the transmission of obscene or objectionable material. Civic society in India is concerned that the culture of blocking at ISPs is curtailing online access to content that is perfectly legal and should be protected by the Indian constitution.

Network Disruptions

Network disruptions are also a major concern in India. In January 2012, during a period of political unrest, telecommunication networks were pre-emptively shut down in Jammu and Kashmir amidst fears that mobile phones could be used to detonate bombs.[13] Beyond the direct disruption of networks, the government engaged in the direct censorship of the media and of expression with local television stations suspended, several Facebook pages taken down, text messages blocked and local newspapers stopped from printing in the city of Srinagar based on their political slant or content.

11 In January 2007, the Department of Telecommunications announced that it would install filtering mechanism at India's international gateways. OpenNet Initiative, 'Country Profile: India' (9 August 2012) https://opennet.net/research/profiles/india accessed on 10 September 2013.
12 Ibid.
13 Freedom House, 'Freedom on the Net 2012: India', http://www.freedomhouse.org/report/freedom-net/2012/india accessed on 9 September 2013.

In August of that year, during riots in the north-eastern states, India banned the sending of bulk SMS messages across the entire country for 15 days and blocked hundreds of websites that allegedly contained inflammatory content to prevent violence.[14] This decision was undertaken without judicial oversight, as national telecom operators had to comply with an executive order from the Home Ministry.[15]

The communal riots in Jammy and Kashmir provoked one of the biggest internal migrations of recent times and fears of escalation led to heavy-handed network disruptions. The disputed territory of Kashmir is frequently the target of such disruptions and encapsulates the complexity of the use of pre-emptive censorship to prevent the very real threat of violence.[16] On the one hand, the traditional media landscape is expanding and the internet has brought new reporting opportunities for citizen journalism. Many Kashmiris now have mobile devices that allow them to capture images and videos and share information. Hundreds of videos have been uploaded and shared on the internet by people in the state. However, during times of political tension, Kashmiris are denied their right to freedom of expression when the government cuts off access to the internet. In February 2013, the Indian government suppressed all news and communications channels – including television stations, newspapers and mobile Internet service – in the Kashmir Valley when Kashmiri militant Mohammad Afzal Guru's execution in New Delhi revived political unrest in the troubled region.[17]

There is evidence to suggest the blocking of cable TV is not just a problem in Kashmir. According to the Asian Media Barometer for India, authorities in a number of states occasionally block certain cable news channels or instruct cable operators not to carry channels based on their political views or content.

The restrictions on digital free speech in India are of great concern. The main issues are takedown and blocking policies, along with the network shutdowns and criminalisation of online speech. Amending notice and takedown procedures are key reforms necessary to provide greater clarity and certainty to intermediaries. Intermediaries should be required to alert authors and provide them a means of appeal when their content is flagged for takedown, a process that can often take longer than 36 hours. The time frame for intermediaries to respond should be extended. Codifying these reforms into law and implementing them swiftly and effectively would reduce the associated threat to freedom of expression.

14 Times of India, '5 SMS per day limit comes into effect' (18 August 2012), http://articles.timesofindia.indiatimes.com/2012-08-18/telecom/33260957_1_smses-and-mmses-bulk-messages-ban-period accessed on 9 September 2013.
15 Ibid.
16 Sumit Galhotra, Committee to Protect Journalists, 'In Indian Kashmir, concerns over Internet censorship' (4 October 2012), http://www.cpj.org/blog/2012/10/in-indian-kashmir-concerns-raised-over-internet-ce.php accessed on 10 September 2013.
17 Reporters Without Borders, 'News media and internet totally censored in Kashmir' (13 February 2013), http://en.rsf.org/india-news-media-and-internet-totally-13-02-2013,44066.html accessed on 10 September 2013.

2 Criminalisation of online speech

The criminalisation of online speech in India is of concern as the authorities have prosecuted legitimate political comment online and personal views expressed on social media. New free speech opportunities offered by social media usage in India have been diminished after the introduction of provision 66A of the IT Act and the arrest of a number of Indian citizens for posting harmless content.[18] This chapter looks at how Section 66A constitutes a significant impediment to freedom of expression and will demonstrate the need to reform the law.

In 2011, Communications Minister Kapil Sibal asked Google, Facebook and Yahoo! to design a mechanism that would pre-filter inflammatory and religiously offensive content.[19] This request was not just, as noted at the time, technologically impossible, it was also a clear assault on free speech. The request demonstrated that even if Section 66A were reformed, further work would still be needed to prevent politically motivated crackdowns on social media usage.

Section 66A of the IT Act is both overly broad and also carries a disproportionate punishment. The section punishes the sending of "any information that is grossly offensive or has menacing character" or any information meant to cause annoyance, inconvenience, obstruction, insult, enmity, hatred

18 BBC News, 'Outrage at India arrests over Facebook post' (20 November 2012), http://www.bbc.co.uk/news/world-asia-india-20405193 accessed on 5 September 2013.
19 The Hindu, 'Sibal warns social websites over objectionable content' (6 December 2011), http://www.thehindu.com/news/national/sibal-warns-social-websites-over-objectionable-content/article2690084.ece accessed on 5 September 2013.

or ill will, among other potential grievances. The provision carries a penalty of up to three years imprisonment and a fine.

> ***IT (Amendment) Act 2008***
>
> 66A: Any person who sends, by means of a computer resource or a communication device,
>
> (a) any information that is grossly offensive or has a menacing character; or
>
> (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or
>
> (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
>
> shall be punishable with imprisonment for a term which may extend to three years and with fine.

Much of the 2008 law historically stems from the 1935 UK Post Office (Amendment) Act, which related to telephone calls and telegraph messages. Rather than update the law to remove this dated provisions, the Indian government decided to extend them to new technologies.

Of particular concern is that there have been a number of arrests made under Section 66A for political criticism on Facebook, Twitter and even via private email. This is a worrying trend that may indicate an intolerance towards public interest speech about politicians that ought to be protected. Criminal and civil cases have also been brought against dozens of internet companies for failing to remove content deemed by some to be defamatory or religiously offensive.[20] Indians new to social media are learning to navigate the red lines of free speech or face prosecution. This degree of censorship is unwelcome in a functioning democracy.

For example, two women were arrested in 2012 for their use of Facebook, one for criticising disruptions in Mumbai during a politician's funeral and the other for "liking" her friend's comment (see case study). The two women were arrested under Section 66A and their arrest soon sparked public outrage, with the Times of India newspaper denouncing "a clear case of abuse of authority" by the police.[21]

20 Freedom House, 'Freedom on the Net 2012: India', http://www.freedomhouse.org/report/freedom-net/2012/india accessed on 9 September 2013.

21 Times of India, 'Shame: 2 girls arrested for harmless online comment' (20 November 2012), http://articles.timesofindia.indiatimes.com/2012-11-20/mumbai/35227016_1_police-station-shiv-sainiks-police-action accessed on 5 September 2013.

Case study: "Facebook arrests"

On Sunday 18 November 2012, a 21-year-old Mumbai woman, Shaheen Dhada, shared her views on Facebook on the shutdown of the city as Shiv Sena chief Bal Thackeray's funeral was being held. Her friend Renu Srinivasan "liked" her post. At 10.30 am the following day, they were both arrested and were ordered by a court to serve 14 days in jail. Hours later, they were eventually allowed out on bail after paying two bonds of Rs. 15,000 (£145) each.

Dhada had posted, "Respect is earned, not given and definitely not forced. Today Mumbai shuts down due to fear and not due to respect". A local Shiv Sena leader filed a police complaint and Dhada and Srinivasan were booked under Section 295 A of the Indian Penal Code (IPC) for "deliberate and malicious acts, intended to outrage religious feelings or any class by insulting its religion or religious beliefs." Subsequently they were also charged under Section 505 (2) of the IPC for making "statements creating or promoting enmity, hatred or ill-will between classes", and the police added Section 66A of the IT Act to the list of charges.

After a significant public outcry, charges were finally dropped. Other recent examples include a 19-year-old, Sunil Vishwakarma, who was detained for a derogatory Facebook post against a politician.[1] "We have received a complaint that he posted some objectionable comments against Raj Thackeray", said an officer at Palghar police station. The police did not charge the teenager. He was questioned and later taken to a special cyber-crime cell before being released. In October 2012, Ravi Srinivasan, a 46-year-old businessman in the southern Indian city of Pondicherry, was arrested for a tweet criticising Karti Chidambaram, the son of Indian Finance Minister P Chadambaram. He was later released on bail.

1 Indian Express, 'Now Palghar police detain 19-year-old for Facebook post on Raj Thackeray' (28 November 2012), http://www.indianexpress.com/news/now-palghar-police-detain-19yrold-for-facebook-post-on-raj-thackeray/1037462/ accessed on 5 September 2013.

Popular outrage over the police's misuse of Section 66A led the Minister for Information and Communication Technology, Kapil Sibal, to issue a guidance to states on how to implement the controversial section of the IT Act.[22] However, there remain ongoing issues relating to political interference in law enforcement itself and to the vague wording of the law itself, with the use of the terms "annoyance" and "inconvenience" overly broad, giving the authorities a wide scope to criminalise comment and opinion.[23]

Despite top-down resistance to change, there is a push for reform of the law. Beyond the guidelines issued in late 2012 to prevent misuse of Section 66A, a revision of the law itself is still needed to prevent warrantless arrests and prosecutions. Civil society and political pressure to reform the law have recently increased. In 2012, cartoonist Aseem Trivedi and journalist Alok Dixit founded Save Your Voice, a movement against internet censorship in India that opposed the IT Act and demands democratic rules for the governance of internet.[24] The Minister for Information and Communication Technology has acknowledged there is an issue over the interpretation of 66A: "It's very difficult to

22 New guidelines require that no less than a police officer of a rank of Deputy Commissioner of Police will be allowed to permit registration of a case under provisions of the Information Technology Act.
23 Some provisions in Section 66A were purportedly drafted to prevent spam – messages typically sent in bulk and unsolicited.
24 Save Your Voice, a movement against web censorship, http://www.saveyourvoice.in/p/about.html

interpret the act on the ground. If you give this power to a sub-inspector of police, it is more than likely to be misused".[25] Yet, he has defended the controversial law and resisted change, justifying his decision by saying that there was "no rampant misuse".[26]

In January 2013, Rajeev Chandrasekhar, member of the upper house of the Indian Parliament, filed a petition to the Indian Supreme Court challenging Section 66A and the Information Technology [Intermediaries Guidelines] Rules for being "arbitrary and uncanalized, […] and in violation of the rights available to citizens under Articles 14, 19 and 21 of the Constitution." Five other petitions related to the IT Act are currently under review by the Supreme Court. The Supreme Court has directed that pleadings will be listed before the Court in the first week of January 2014. This is a welcome step but the Supreme Court must deal with these cases as a matter of urgency and even in the case of success for the petitions, these decisions will require political will to be implemented.

The criminalisation of online speech and social media usage is a serious threat to freedom of expression in the country. The use of "offence" to silence political criticism online jeopardises free speech as a fundamental right necessary for public debate in a democracy. It is clear that there is the need and the public will to reform the law. The arrests and prosecution of citizens for innocuous messages has tarnished India's image as the world's largest democracy. While the 2014 General Elections offer a window of opportunity for change, the Indian authorities must undertake reform of the IT Act and end resistance to change.

25 Lakshmi Chaudhry, First Post, 'The real Sibal's law: Resisting Section 66A is futile', http://www.firstpost.com/politics/the-real-sibals-law-resisting-section-66a-is-futile-541045.html?utm_source=ref_article accessed on 18 November 2013.
26 Nikhil Pahwa, Medianama, News and Analysis of Digital Media in India, 'Sibal defends IT Act Section 66A in Parliament: Notes', http://www.medianama.com/2012/12/223-sibal-defends-it-act-section-66a-in-parliament-notes/ accessed on 18 November 2013.

3 Surveillance, privacy and government's access to individuals' online data

Recent revelations in the Hindu have raised concerns over the extraordinary extent of domestic surveillance online, without any legal and procedural framework to protect privacy.[27] This chapter looks at how the Indian government's surveillance and access to individuals' online data presents a threat to freedom of expression. When people know or assume that governments or companies are monitoring their private communications, they are less inclined and less likely to communicate freely. The UN's Special Rapporteur on Freedom of Expression Frank La Rue delivered a report to the Human Rights Council outlining how state and corporate surveillance undermine freedom of expression and privacy.[28] His report states that "Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other."

At the end of 2012, major telecom companies in India agreed to grant the government real-time interception capabilities for the country's one million BlackBerry users. The Indian government has consistently requested that major web companies set up servers in India to allow them to monitor local communications.[29] Such surveillance capabilities potentially breach international human rights standards and have been subject to court challenges. In 1996, the Indian Supreme Court held that the citizen's privacy has to be protected from abuse by the authorities.[30] Yet, Section 69 of the IT Act gives the state surveillance powers in the interest of national security or "friendly relations with foreign states".[31]

In April 2013, India began implementing a $75 million Central Monitoring System (CMS) that will allow the government to access all digital communications and telecommunications in the country.[32] Content covered by the CMS will include all online activities, phone calls, text messages and even social media conversations. The scope of the programme, in development since 2009, is still to be determined, but some worry about the lack of safeguards against abuse in its implementation. Pranesh Prakash, Policy Director at the Centre for Internet and Society, argues: "In India, we have a strange mix of great amounts of transparency and very little accountability when it comes to surveillance and intelligence agencies."[33]

Opponents of the system and human rights advocates worry the government will abuse the CMS to monitor or arrest political critics rather than to enhance national security as intended.[34] Arguably, CMS may violate Article 21 of the Constitution guaranteeing "personal liberty". Concerns remain that without comprehensive privacy laws in India, the system will not be sufficiently accountable, and could chill free expression. Cynthia Wong, senior Internet researcher at Human Rights Watch, says: "The Indian government's centralized monitoring is chilling, given its reckless and irresponsible use of the sedition and Internet laws. New surveillance capabilities have been used around the world to target critics, journalists, and human rights activists."

---

27 Shalini Singh, The Hindu, 'India's surveillance project may be as lethal as PRISM' (21 June 2013), http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece accessed on 24 September 2013.

28 Brian Pellot, Index on Censorship, 'UN report slams government surveillance', http://www.indexoncensorship.org/2013/06/government-surveillance-apple-google-verizon-facebook/ accessed on 10 September 2013.

29 Firstpost, 'Telecos agree to real-time intercept for Blackberry messages' (31 December 2012), http://www.firstpost.com/tech/telecos-agree-to-real-time-intercept-for-blackberry-messages-573612.html accessed on 10 September 2013.

30 Pranesh Prakash, New York Times, India Ink (blog), 'How Surveillance Works In India' (10 July 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0 accessed on 10 September 2013.

31 The Information Technology Act, Amendment, 2008, Section 69, 'Directions of Controller to a subscriber to extend facilities to decrypt information', http://cca.gov.in/cca/sites/default/files/files/itact-amendments2009.pdf accessed on 23 September 2013.

32 Times of India, 'Government can now snoop on your SMSs, online chats' (7 May 2013), http://timesofindia.indiatimes.com/tech/tech-news/internet/Government-can-now-snoop-on-your-SMSs-online-chats/articleshow/19932484.cms accessed on 5 September 2013.

33 Pranesh Prakash, New York Times, India Ink (blog), 'How Surveillance Works In India' (10 July 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0 accessed on 10 September 2013.

34 Mahima Kaul, Index on Censorship, 'India's plan to monitor web raises concerns over privacy', http://www.indexoncensorship.org/2013/05/indias-plan-to-monitor-web-raises-concerns-over-privacy/ accessed on 5 September 2013.

In addition, new laws passed in April 2011 expanded internet surveillance in cybercafés, the primary point of access for the majority of Indians who cannot afford private computers or smartphones (see the section on access). Furthermore, Indians are required to register their real names to activate SIM cards and mobile and internet service providers (ISPs) are required to grant government authorities access to user data. Requesting user data becomes problematic when data is used for prosecuting free speech online and stifling political criticism (see section on criminalisation of online speech and social media).

India is one of the worst offenders globally both for takedown and for user requests, though on user information it is ranked after the US. The Google Transparency Report shows that India ranks second – after the United States – in the number of government requests for users data.[35] In August 2013, Facebook released a similar report. During the first six months of 2013, India ranks second in number of total requests (3,245 requests) and Facebook produced data in 50 percent of the cases.[36] It is possible that data requested by the government will be used in criminal prosecutions for defamation, hate speech, or harming "communal harmony". This is problematic because these laws in themselves are too vague and broad and do not protect freedom of expression adequately, resulting in disproportionate arrests and prosecutions merely for the expression of views on a blog, liking a post on Facebook, or writing a political tweet. Without privacy law and safeguards to protect data, the collection and retention of such data can be misused and generate a chilling effect among the Indian population.

Many Indian MPs are aware of the need for a legal framework to protect the privacy of Indian citizens. In 2011, Parliament passed new data protection rules, but there is still no privacy law in India. Privacy is a fundamental human right and underpins human dignity and other key values such as freedom of association and freedom of expression. Key changes suggested by internet advocates include a Privacy Bill to address data protection and surveillance, and the establishment of a Privacy Commission.[37] It is time for the Indian government to take better account of the right to privacy and protection from arbitrary interference with one's privacy.[38] Addressing mass surveillance and unwarranted digital intrusions in India are both necessary steps to fight self-censorship and promote freedom of expression.

35 Google, 'Google Transparency Report', http://www.google.com/transparencyreport/userdatarequests/IN/ accessed on 5 September 2013 and 15 November 2013.

36 Facebook, 'Global Government Requests Report', https://www.facebook.com/about/government_requests accessed on 5 September 2013.

37 In 2013, the Centre for Internet and Society drafted a Privacy Bill addressing data protection, surveillance and interception of communications. Centre for Internet and Society, 'Privacy (Protection) Bill, 2013: Updated Third Draft' (30 September 2013), http://cis-india.org/internet-governance/blog/privacy-protection-bill-2013-updated-third-draft accessed on 4 October 2013.

38 The Universal Declaration of Human Rights, Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." http://www.un.org/en/documents/udhr/

4 Access: Obstacles and opportunities

Key concerns in assessing online freedom of expression in India are the barriers to accessing the internet itself. There are a number of major obstacles to online access in India namely infrastructural limitations, cost considerations as well as illiteracy and language. In addition, this section argues that security considerations have created further barriers for Indian people to access the internet.

With around 120 million web users – 12.6 percent of India's population – internet penetration is relatively low by global standards. Yet as cheaper smartphones enable millions more to access the net, usage is increasing and the government is prioritising digital access and development as a political objective. Digital access initiatives are being developed in India to fight illiteracy and poverty, promote Indian language content online, increase broadband penetration and speed in rural and urban areas, and improve the reliability of electricity.[39]

In May 2006, the government approved a National e-Governance Plan to implement national e-governance with the aim to make all government services accessible to localities. This project aims to connect more Indian citizens through the National Optic Fibre Network and takes into account the need to increase internet access in the country.[40]

One of the major barriers to access online content is language. There are 22 primary regional languages in India, but most online content is in English, a language only 11 percent of the population can read.[41] Civil society initiatives have moved quicker than the government. Journalist Shubhranshu

39 Hari Kumar, New York Times, India Ink (Blog), 'In India Homes, Phones and Electricity on Rise but Sanitation and Internet Lagging' (14 March 2012), http://india.blogs.nytimes.com/2012/03/14/in-indian-homes-phones-electricity-on-rise-but-sanitation-internet-lagging/ accessed on 11 September 2013.

40 Government of India, National e-Governance Plan, http://india.gov.in/e-governance/national-e-governance-plan

41 OpenNet Initiative, 'Country Profile: India' (9 August 2012) https://opennet.net/research/profiles/india accessed on 10 September

Choudhary has created the news platform CGNet Swara, which lets people use their mobile phone to listen to and leave their own stories, bringing news to communities who don't speak Hindi or English, and are therefore denied access to mainstream newspapers or news websites.[42]

Broadband access and the price remains a major barrier to digital freedom of expression with only 3% of households having a fixed internet connection in 2012.[43] For this reason, many Indian users access the internet via cybercafés. However in 2011, fearing that cybercafés facilitated criminal and terrorist activities, the Indian Government introduced strict rules restricting cybercafés under Section 79 of the IT Act.

Many have denounced the cybercafé rules as restricting access to cybercafés and infringing Indian citizen's freedom of expression and privacy rights.[44] The rules are problematic in many ways. Firstly, they limit the creation and sustainability of cybercafés by imposing draconian administrative requirements. For example, cybercafés must also have the capacity to retain user identity information and the log register in a secure manner for a minimum period of a year. Secondly, the rules directly limit citizens' access to cybercafés. Cybercafés cannot allow users to use computer resources without providing an established identity document, a barrier for poorer people in rural communities who are disproportionately likely not to have the required identification.

India faces numerous obstacles to internet access, from infrastructural limitations to costs and language restrictions.[45] While government efforts to increase broadband penetration and speed in rural and urban areas are welcome, restrictions on access to and the functioning of cybercafés must be lifted.

2013.

42 Rachael Jolley, Index on Censorship, 'India calling', 'Not heard? Ignored, suppressed and censored voices', Volume 42, Number 03, September 2013.

43 Hari Kumar, New York Times, India Ink (Blog), 'In India Homes, Phones and Electricity on Rise but Sanitation and Internet Lagging' (14 March 2012), http://india.blogs.nytimes.com/2012/03/14/in-indian-homes-phones-electricity-on-rise-but-sanitation-internet-lagging/ accessed on 11 September 2013.

44 Information Technology [Guidelines for Cybercafés] Rules, 2011, http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf accessed on 11 September 2013.

45 Freedom House, 'Freedom on the net 2013', http://www.freedomhouse.org/report/freedom-net/2013/india accessed on 4 October 2013.

5 India's role in global internet debates

International summits and fora over the next two years will be critical in determining the internet's future. The open and inclusive multistakeholder model of internet governance has been called into question, with some governments – namely China, Iran and Russia – advocating for more control. As an influential state in our increasingly digital and multipolar world, India has the opportunity to push policies that promote digital freedom. Yet, India is still very much a swing state in these internet governance debates.

After initial scepticism, India has now joined the European Union (EU) and the US in resisting the call for a top-down government-led approach for global internet governance. At the World Conference on International Telecommunication in Dubai in December 2012, India was one of the few countries to side with EU member states and the US in supporting the current multistakeholder status quo. This was the result of a debate in India, in which the key battle line was whether internet freedom constituted a daunting threat to security that required top-down national control or not.

India's hesitation increased after the 2008 Mumbai attacks when Jaider Singh, Secretary of the Department of Information Technology, described the internet as "both a vehicle and a target of criminal minds".[46] Concerns over security and spam led India to advocate for more national control over internet governance, through the creation of a United Nations committee.[47] Earlier in 2011 at the Internet Governance Forum in Nairobi, India, along with South Africa and Brazil - two other crucial swing states in the internet governance debate – proposed a similar initiative.

While such top-down control has long been advocated by the likes of China and Iran – countries with a poor domestic track record on digital freedom – it is a direct threat to internet openness and the exercise of human rights online by placing too much control of the process in the hands of national governments. The EU and US tried to address India's concerns diplomatically by agreeing to a working group.

It is positive that India is now willing to play an important role in defending the multistakeholder model of internet governance against calls for more top-down state regulation. Yet, it is clear that with a sixth of the world's population, it is not just important for India's government to defend internet freedom globally, but also ensure that its domestic record stands up to scrutiny and is a model for the rest of the world to adopt. Currently, this is not the case.

India is not only setting internet policies for its 10 percent of users today, but for its 1 billion citizens yet to come online. The decisions it makes, both domestically and on the international stage, are likely to set powerful precedents for regional neighbours, and other emerging democratic powers.

---

46 Jaider Singh, speaking at the third annual Internet Governance Forum in Hyderabad, India, in 2008 with the theme 'Internet for All.' Internet Governance Forum, 'Internet Governance Forum Concludes Hyderabad Meeting' (6 December 2008), http://www.elon.edu/docs/e-web/predictions/IGF 08 Daily Highlights Dec 6.pdf accessed on 10 September 2013.

47 In 2011, India proposed a United Nations Committee for Internet-Related Policies (CIPR) be established to develop and oversee internet policies that would affect the world's users. Techdirt, 'India Want UN Body To Run The Internet: Would That Be Such A Bad Thing?' (2 November 2011), http://www.techdirt.com/articles/20111102/04561716601/india-wants-un-body-to-run-internet-would-that-be-such-bad-thing.shtml accessed on 2 September 2013.

Conclusion

This paper has shown that despite its lively democracy, strong tradition of press freedom and political debates, India is in many ways struggling to find the right balance between freedom of expression online and other concerns such as security. While civil society is becoming increasingly vocal in attempting to push this balance towards freedom of expression, the government seems unwilling or unable to reform the law at the speed required to keep pace with new technologies, in particular the explosion in social media use. The report has found the main problems that need to be tackled are online censorship through takedown requests, filtering and blocking and the criminalisation of online speech.

Politically motivated takedown requests and network disruptions are significant violations of the right to freedom of expression. The government continues its regime of internet filtering and the authorities have stepped up surveillance online and put pressure on internet service providers to collude in the filtering and blocking of content which may be perfectly legitimate.

Despite numerous calls for change, the government has refused to reform the controversial IT Act. However, public outrage and protests against abuses of the law have multiplied since 2012. Civil society and political initiatives against this legislation have increased and demands for new transparent and participatory processes for making internet policy have gained popular support.

Technical means designed to curb freedom of expression, arguably to achieve political gain, have no place in a functioning democratic society. While government efforts to expand digital access across the country are promising, these efforts should not be undermined by disproportionate and politically motivated network shutdowns.

While it is to be welcomed that India is taking a more vocal part in the global internet governance debate in favour of the multistakeholder approach, it is essential it ensures its own laws are proportionate and protect freedom of expression in order for the country to have the most impact in this debate.

To end internet censorship and provide a safe space for digital freedom, Indian authorities must:

- Stop prosecuting citizens who express legitimate opinions in online debates, posts and discussions;
- Revise takedown procedures, so that demands for online content to be removed do not apply to legitimate expression of opinions or content in the public interest, so not to undermine freedom of expression;
- Reform IT Act provisions 66A and 79 and takedown procedures so that content authors are notified and offered the opportunity to appeal takedown requests before censorship occurs;
- Stop issuing takedown requests without court orders, an increasingly common procedure;
- Lift restrictions on access to and functioning of cybercafés;
- Take better account of the right to privacy and end unwarranted digital intrusions and interference with citizens' online communications;
- Maintain their support for a multistakeholder approach to global internet governance.

Xindex

the voice of free expression