

BREAKING THE WALLS:

THE FIGHT FOR FREEDOM OF EXPRESSION IN THE DIGITAL SPACE IN SOUTH ASIA

UNDEF The United Nations Democracy Fund

IFJ FIP

May 2016

This document has been produced by the International Federation of Journalists (IFJ) on behalf of the South Asia Media Solidarity Network (SAMSN).
Afghan Independent Journalists' Association
All India Newspapers Employees' Federation
Bangladesh Manobadhikar Sangbadik Forum
Federation of Nepali Journalists
Free Media Movement, Sri Lanka
Indian Journalists' Union
Journalists Association of Bhutan
Maldives Journalists' Association
National union of Journalists, India
National Union of Journalists, Nepal
Nepal Press Union
Pakistan Federal Union of Journalists
Sri Lanka Working Journalists' Association
South Asia Media Solidarity Network (SAMSN) – Defending rights of journalists and freedom of expression in South Asia.
samsn.ifj.org/
The SAMSN Digital Hub – https://samsn.ifj.org/map/ provides a listing of all known cases of media rights violations from 2014.

Author: Christopher Warren
Sub-editor: Sukumar Muralidharan
Editorial Support:
Alexandra Hearne
Jane Worthington
Ujjwal Acharya
Contributors:
Sunanda Deshapriya
Lucy Purdon
Designed by: Magnesium Media

Images: Photographs are contributed by IFJ affiliates and also accessed under a Creative Commons Attribution Non-Commercial Licence and are acknowledged as such through this report.

Cover Artwork: 'Disturbance detected' by Indian political cartoonist and activist Aseem Trivedi. Read more on page 8.

This document has been produced with support from the United Nations Educational, Scientific and Cultural Organisation (UNESCO); United Nations Democracy Fund (UNDEF) and the Norwegian Ministry of Foreign Affairs (NMFA). The views and contents expressed herein are those of the IFJ and can in no way be taken to reflect the official opinion of UNESCO, UNDEF and NMFA.

The author will be responsible for the choice and presentation of the facts contained in the paper and for the opinions expressed therein, which will not be necessarily those of UNESCO, UNDEF and NMDA and do not commit the Organisations, the designations employed and the presentation of material throughout this book will not imply the expression of any opinion whatsoever on the part of UNESCO, UNDEF and NMFA concerning the legal status of any country, territory, city or area, or its authorities or concerning the delimitation of its frontiers and boundaries.

MOBILE VOICES

FREEDOM OF SPEECH IN MOBILE PLATFORMS IN SOUTH ASIA

Freedom of expression in the digital space across South Asia is at a pivotal point. The expansion of broadband access and mobile technology has created exciting opportunities for journalists to inform communities and to empower new voices and report in new ways.

At the same time, the expansion of access to the internet has generated increasing attempts to control discussion and debate and to exclude dissident voices. Official efforts at controlling the new discourse on the social media continue – often without a legal mandate – while non-state actors pose another manner of threat to free speech in the digital space. Journalists, writers and campaigners working in the digital space have faced a broad range of potential censors – governments themselves, political groups, military and para-military groups, religious extremists, criminal gangs and terrorist organisations. At times these groups have overlapped in a way that has intensified threats to the diverse freedoms the internet should be able to deliver.



Credit: STRDEL/AFP

As media and journalists adapt to the leap to mobile internet platforms, South Asia's governments respond with restrictions that silence freedom of expression.



Credit: Munir Uz Zaman/AFP

Since 2013, seven secular online bloggers have been hacked to death in Bangladesh. Following the murders, protests have been held across Bangladesh calling for the government to guarantee freedom of expression.

THE RISE OF THE SOCIAL INTERNET

South Asia is in the midst of a surge in expansion of the internet. Rather than replicating step by step the on-line progress of the developed world, South Asia is leaping straight to a world dominated by social media platforms accessed through mobile devices. Rather than a world of URLs, bulletin boards and emails, South Asia is leaping to a world of social media platforms and smart phones, bypassing web pages and landlines. This means most citizens are coming straight from an almost pre-internet society to the most advance communication paradigm that prioritises social media platforms delivered and accessed through mobile.

This is transforming the region, particularly in the urban conglomerations. And it is forcing governments, journalists and the on-line community to adapt.

Of course, most South Asian countries had access to the internet from the mid-nineties. But the slow development of broad band – which remains relatively limited even today – meant that the shift of media – and media advertising – on-line that occurred quickly in the developed world has been much slower in south Asia.

The internet arrived in South Asia at a time when many communities had limited access to even basic telephony. For example, according to a recent report by the Central Bank of Sri Lanka, "teledensity" or connections per person has jumped in 20 years from one per 100 in 1995, to 107 per hundred. In 1998, the World Bank admitted that there were five times as many people using the internet inside the bank than in the entire population of Bangladesh.

Now, one in three people in Bangladesh are estimated to have internet access.

This was part of what was referred to at the time as the digital divide – a fear that the information society would entrench economic and social disadvantage between the developed and the developing world. Most famously, South African President Thabo Mbeki popularised this view in 2001 when he repeated an early 1990s quote from *The Economist* magazine that half the world's population had never made a phone call.

There were pockets of early development in south Asia, almost all in urban areas. The best known of these was the development of two south Indian cities, Bangalore and Hyderabad, as global hubs of the information technology (IT) industry. Enterprises in both these cities developed state of the art communications to link with customers and principals based abroad, but did not seem to catalyse much of a growth of the internet within their neighbourhoods. Despite the patchy progress achieved in certain locations, notably in India, South Asia as a whole had limited access.

This century, South Asia has been racing to catch up. To take the case of India alone. It was estimated that by the turn of the century, a new mobile telephone connection had become considerably cheaper to create than a new landline connection. In 2000, the number of landline connections was roughly fifteen times more than the number of active mobile connections. By 2005, mobile connections had outstripped

landlines. They have since continued to grow rapidly and today the number of mobile phones is of the same order of magnitude as India's billion plus population, while wireline connections have stagnated at about 30 million.

Internet access has jumped from about 3 per cent of the population in 2000 to about 30 per cent today across the region. And the mobile net is providing the runway for South Asia to leapfrog to effective universal access by 2020. It is likely that most of South Asia will simply bypass the traditional land-line based internet to the mobile internet. The increasing bandwidth and speed of transmission through mobile phone networks makes it a very real possibility that South Asia could in large measure bypass the wireline stage in communications.

A major contributor to this leapfrogging has been the spread of smart phones. According to the Pew Research Centre global survey, by 2015, 17 per cent of the Indian population had smart phones. Similarly, in Pakistan, 11 per cent of the population had smart phones. In countries like Sri Lanka and Bangladesh it was less than 10 per cent.

These figures, of course, skew towards the young, the better off and the better educated. For example, according to Pew, 27 per cent of Indians aged 18-34 use a smartphone and in Pakistan 13 per cent. Nonetheless, it is estimated that the Asia-Pacific will be one of the drivers of the spread of smart phones over the next four years, which will result in mobile being the dominant source of internet data. (http://www.ericsson.com/news/1925907)

At the same time, people in South Asia have embraced social media. One source estimates that about one in every eight people in South Asia is on FaceBook (worldinternetstats) and, according to *The Economic Times*, India on its own is on target to become the largest national user of Facebook, with the overwhelming majority using mobile devices for access.

Volume of numbers means the most popular figures on Twitter are almost all from South Asia either as politicians, such as Indian Prime Minister Narendra Modi, film star Deepika Padukone or cricketer Virat Kohli, all with followers in the millions.

As the citizens of South Asia embrace the opportunities of access to information that the mobile web provides, journalists and other content creators are grasping the opportunity to inform and entertain their communities through mobile platforms. At the same time, governments, politicians, terrorists and criminal gangs are threatening the ability of journalists to do their job in ensuring our communities get the sort of information they are demanding.

SHUTTING DOWN THE NET

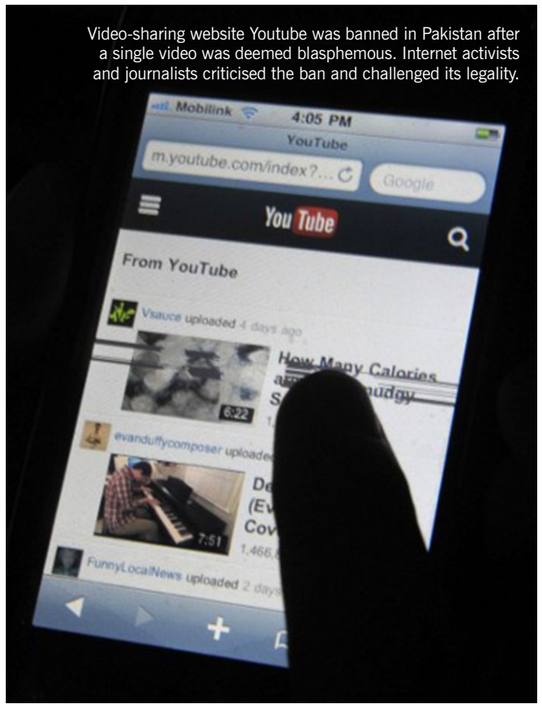
The expansion of the internet in South Asia has been matched with an engagement by governments to censor content on the net through measures, ranging from total shutdowns of the web, through to the imposition of filtering requirements on Internet Service Providers.

Governments in South Asia have led the world in imposing total shutdowns either on a national or state wide basis. Although this is generally justified on "national security"



Nepalese journalists hit back after the country's military shut down all internet and telecommunications as part of the 2005 royal coup. The Federation of Nepali Journalists (FNJ) called the restrictions an attack on freedom of expression.

Credit: Devendra M Singh/AFP



Video-sharing website Youtube was banned in Pakistan after a single video was deemed blasphemous. Internet activists and journalists criticised the ban and challenged its legality.

Credit: Banaras Khan/AFP

grounds, there can be no doubt that many of the closures have been driven by political or other considerations and many have been imposed with no clear legal mandate.

Major shutdowns in South Asia have included:

In February 2005, as part of the royal coup in Nepal, the military shut down all internet and telecommunications services. This included landlines, mobile networks and the internet. For about two weeks, the only means of communication were short-wave radio and satellite phones.

In Pakistan, shutdowns of the mobile network began in Balochistan in 2005 and from 2012 were expanded to towns – and on occasions entire regions – across the country. There are reports of up to 14 full or partial shutdowns of the mobile phone networks in 2012 and 2013, although bytesforall, which documents the closures say these have eased since the change of government later that year. Sometimes the trigger for these events was a genuine terrorist attack or riot. Other times, they were imposed as pre-emptive measures to religious festivals or political rallies.

Shutdowns have occurred in 2010 and 2011 over content deemed derogatory to the Islamic faith. The matter has been litigated in the higher judiciary in Pakistan, though a final verdict is yet to be pronounced.

To monitor the continued shut downs, bytesforall launched a dedicated web site called killswitch.pk to track the shutdowns. This shows that in 2015, the Pakistani government was shutting down mobile services for each of the major public holidays as a precautionary measure.

In India, Internet Shutdown Tracker by the Software Freedom Law Center (SFLC) lists 13 instances of internet shutdown in India since 2013. internet shutdowns, especially through the mobile network have been a common occurrence in the Kashmir region of Jammu and Kashmir state, which has suffered close to a quarter century of insurgency. Every observance of an event of significance in the Indian nationalist calendar usually involves a partial or complete shutdown of internet access in Kashmir, to prevent word getting around about plans to disrupt official events. Specific instances of a shutdown of the internet in recent times include:

- **Kashmir:** In March 17-18, 2014, the internet was shut down to prevent Kashmiri leaders linking by on-line video to a side-event at the Human Rights Commissions in Geneva. Internet services were cut off when Prime Minister Narendra Modi visited Kashmir in November 2015. A similar disruption occurred for three days in October, when there was an apprehension of communal strife, after a Hindu nationalist party with a strong base in the Jammu region exerted its influence as a member of the ruling coalition in the state, to impose a ban on the sale and consumption of beef in Kashmir.
- **Gujarat:** Mobile data and SMS was shut off in the town of Vadadora, the third largest city in Gujarat, in September 2014, after a FaceBook post that was said to "hurt religious sentiments". Mobile internet in the region was again suspended in late August 2015 to stop discussion and "rumours" on social media such as WhatsApp and Facebook, after widespread public disturbances caused by a communal organisation's agitation for inclusion in affirmative action programmes of the state and central governments.
- **Nagaland:** internet across the state was shut down in March 2015 to block distribution of a video of a lynching.
- **Manipur:** In September 2015, FaceBook and WhatsApp were blocked amidst agitation over a state legislation that sought to define entitlements to citizenship rights in terms of ethnicity.

Most shutdowns according to the SFLC are ordered under article 144 of the Indian Penal Code, which empowers local authorities to issue prohibitory orders to deal with situations of potential unrest. Early in 2016, the SFLC and a few associated bodies filed a petition in India's Supreme Court asking for this manner of shutdown to be declared unlawful. The Supreme Court though, did not entertain the petition, holding that this manner of curb is permissible in situations of imminent social disorder.

In November, 2015, Bangladesh cut off internet for a few hours later admitting it was a mistakenly done. Messaging apps such as Viber, WhatsApp and others were shut down for weeks for security reasons surrounding war crimes trials at least on three occasions – 22 days in November, 2015; in December, 2015 and January 2016.

The use of the kill switch has serious impacts on the millions of citizens and businesses in South Asia who rely on the internet. The focus on shutting down mobile networks has serious ramifications in a region where an increasing proportion of internet access is through mobile devices.

NETWORK SHUTDOWNS

Network shutdowns first came to global attention during the Arab Spring in 2011, when large parts of Egypt's mobile and internet networks were shut down to dispel the protests. The problem has not gone away. It has gotten worse.

In 2014 & 2015 alone, various sources reported shutdowns in Algeria, Bangladesh, Brazil, Burundi, Central African Republic, Congo-Brazzaville, Democratic Republic of Congo, Ecuador, Iraq, India, Lebanon, Malaysia, Nauru, Niger, North Korea, Pakistan, Somalia, South Sudan, Togo, Turkey, Uganda & Yemen. It varies from large scale mobile and internet network shutdowns in Pakistan for national security reasons, to brief shutdowns of particular services like SMS or social media around elections and protests in the DRC and Burundi. At times a particular service like Whatsapp will be shut down, such as in India to combat the spread of "rumours".

The impact on the people is great. Shutdowns silence large parts of society. This is a significant challenge to freedom of expression and association in modern digital societies increasingly dependent on mobile phone and internet networks. It is often not possible to contact ambulance, police or fire services during these shutdowns. People are cut off from public services such as banking, business & educational applications.

Pakistan suffers the most documented shutdowns in the world. Through Bytes for All's killswitch.pk project, we documented 26 shutdowns since 2012, affecting large areas of the country. In 2015, we jointly wrote a report with the Institute for Human Rights and Business (IHRB) in London and the Centre for Internet and Human Rights (CIHR) in Berlin that conducted research into a mobile network shutdown in Islamabad and Rawalpindi.

This documentation is important because this practice has mostly been allowed to continue unchallenged globally. There is no transparency or accountability as a result of which states do not change their behaviour. Without shining a light on this practice globally, there is little opportunity to understand the avenues for prevention, mitigation and redress.

Lucy Purdon, Bytesforall.pk

Credit: Noah Seelam/ AFP



India's Hyderabad is a global hub of information technology. While much of South Asia still has limited broadband, centres like Hyderabad are moving ahead fast.

FILTERING

Most countries in South Asia also severely limit the free flow of information over the internet through various systems of internet blocking and filtering. In the major countries, legislation gives the relevant authorities wide powers to filter or otherwise ban content on grounds of obscenity, national security, blasphemy or the broader rubric of giving offence, usually on either religious or national grounds.

The rise and popularity of social media sites as tools both for spreading information and one-to-one (or one-to-several) communication has meant that filtering has become a major obstacle to the free flow of information and to basic communication between people.

Reports by open internet advocates suggest that filtering is carried out in India, Pakistan and Bangladesh both through algorithms that identify suspect sites and by direct instruction to ban particular sites or domain names. Increasingly, the filtering powers are being used to block social media sites including Facebook, WhatsApp, YouTube and Reddit either for particular content or to prevent the use of these sites for peer to peer communication.

Filtering is also being used, particularly in Pakistan and India, to target pirate or torrenting sites.

In Pakistan, filtering is done by Internet Service Providers at the instruction the Pakistan Telecommunications Authority. A 2013 report by Citizens Lab at the University of Toronto in Canada found that the Canadian product Netsweeper had been installed on the network of the major telecommunications company, the Pakistan Telecommunications Company Ltd (PTCL) which also operates the Pakistan Internet Exchange through which almost all ISPs in Pakistan access the net.

The Netsweeper technology was being used to filter a broad range of sites including independent media, secessionist organisations as well as sites thought to be religiously offensive. Citizens Lab also found that ISPs were being instructed by the PTA to implement DNS tampering . This means that sites are blocked at the level of the domain name, meaning accessing any pages at that domain will return an error message.

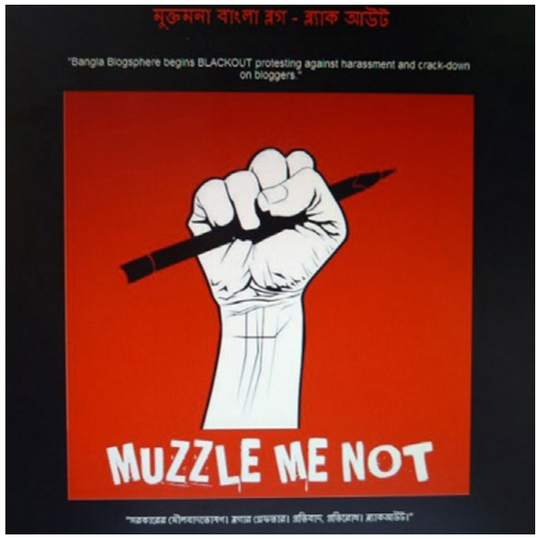
The application of these practices to social media has resulted in the effective banning of the most popular parts of the mobile internet.

The most notorious ban in Pakistan has been on YouTube. This illustrates the challenges and damage that filtering does in the age of social media. After the Supreme Court ordered the blocking of a US video deemed blasphemous, the entire video-sharing website was blocked in September 2012. The regulator said that the only way it could ensure the one video was blocked was by blocking all of You Tube.

In response to this, in 2014, both Twitter and Facebook agreed to self-restrict offensive content in Pakistan, but were forced to backtrack in response to campaigns by users.

Civil rights groups in Pakistan, particularly organisations such as Bolo Bhi and bytesfor all, campaigned against the YouTube ban including court action to challenge the legality of the censorship regulations and its broadbrush application. In January 2016, the ban was lifted only after YouTube agreed to establish a Pakistan specific domain. Neither the Pakistan

Credit: Kamrul Hasan Khan/AFP



An off-line webpage in Dhaka on April 4, 2013. Top Bangladeshi blogs blacked out their sites to protest continuing attacks from radical Islamists.

authorities nor Google have revealed the conditions for the grant of access to this domain.

In India, filtering is carried out by ISPs on instructions from the Department of Telecommunications. This is reinforced by including a requirement to apply filtering in the licensing arrangements with ISPs. The primary justification of filtering has been to restrict pornography (particularly pornography that is also deemed blasphemous). However, it has been used on grounds of social order and to repress political dissent, particularly secessionist dissent.

The Indian authorities have grappled with the challenge of how to apply filtering to social media platforms. For example, as early as 2006, entire blogging platforms, such as Typepad and Blogspot, were blocked to target a handful of dissident blogs. This has been repeated in different states, usually by executive action or through compliant courts.

Government failure to understand how the social internet works has deepened the challenge. Most famously, in December 2011, Telecom Minister Kapil Sibal asked the major social media platforms including Google and Facebook to have humans screen each individual bit of content before posting. This generated social media kickback under the hashtag #idiotkapilsibal..

The government of India has continued to request or direct the social media platforms to withdraw or block certain material in India and has continued to issue instructions to ISPs to block certain URLs, including those that are part of broader networks. This has included orders to block the Internet Archive's *Wayback Machine* site and the video streaming site Vimeo allegedly because they contained pro-terrorist materials.

Faceboook's transparency report says that it restricted about 15,000 items in India in the second half of 2015. Google's transparency report says that in the first six months of 2015 it was asked to remove 1,037 items from Google.in, the overwhelming majority requests coming from police or other authorities.

In 2012, Anonymous hacked one of the major ISPs in India and subsequently publicised the names of sites that had been blocked. The list revealed that the ISP was blocking sites on its own account as well as under orders from the government and courts.

The relationship between the government of India and Facebook was complicated by Facebook's lobbying of the Modi government to be allowed to launch its advertising supported internet access service, internet.org. This was one among two internet services offered free in 2015, but then put on hold as the telecommunications regulator in India initiated consultations to test public opinion. Facebook meanwhile recast its plan in association with a leading Indian telecom operator and launched it under the title "Free Basics". In February 2016, the telecom sector regulator in India disallowed any kind of "differential pricing" of internet services. It held that increased access was a desirable end, but price differentiation would end the internet as "a neutral end-to-end carrier of information", investing service providers with gate-keeping powers. This would "restrict consumer choice" and work against "free speech and media pluralism".

In Bangladesh, there does not appear to be any mandated national filtering scheme in place. Instead, the Bangladesh Telecommunication Regulatory Commission (BTRC) relies on pre-existing laws relating to offensive behaviour, defamation and national security to require ISPs to block certain sites. And, in late 2015, the Press Information Department said it was requiring all on-line news sites to apply for registration or re-registration.

As in Pakistan and India, the authorities have grappled with the challenges of how to block specific social media content without blocking the entire platform. In 2012, Bangladesh joined with Pakistan in blocking access to YouTube over an anti-Islam video. The slower spread of the mobile internet (marked by the slower take up of smart phones) has meant there have been fewer instances of platform wide bans. However, in late 2015, the government blocked Facebook, Twitter and messaging apps including Viber and WhatsApp in an attempt to restrict civil unrest over the death penalties imposed on opposition leaders for war crimes in the 1971 war of liberation.

In a final example, WhatsApp groups in Kashmir are now required to be a licence, with the group administrator liable for any comments in the group.

There is also some evidence that *de facto* filtering is achieved in Bangladesh by throttling internet speeds to restrict access to bandwidth heavy services such as video.

In Sri Lanka, the government elected in January 2015 promised to abandon the almost routine blocking of dissident and exile sites. About 100 pornography sites were blocked on court order in 2010 followed by five news sites in 2011 and a futher two in 2014. By May 2015, it had lifted all restrictions, including those imposed on Tamil voices such as Tamilnet. Certain pornography sites remain blocked.

Despite the lifting of the blocks, journalists and activists remain concerned at government proposals announced this year to to introduce mandatory web registration despite the lack



Credit: STRDEL/AFP

Indian political cartoonist Aseem Trivedi was charged under the notorious Section 66A of India's Information Technology Act in 2012 for a series of cartoons on corruption in India. Trivedi was jailed for two weeks before charges were dropped. Section 66A was struck down by the Indian Supreme Court in 2015.

of legislative authority to do so. This threatens to re-introduce filtering through the back door.

In Nepal the Nepal Telecomm Authority, which issues licences to ISPs, has given directives to block websites, most notoriously in 2010. During an interview in 2016, the chairman of ISP Association of Nepal said that still 'around 100 websites remained blocked by ISPs in Nepal' following the NTA orders.

During Nepal Earthquake in April, 2015, the Nepal Police ordered blocking of some news items that were spreading rumors about earthquake; and briefly detained some reporters.

There have been at least four cases reported of websites being blocked in the Maldives of some cases of news sites being blocked in both Bhutan and Afghanistan.

MAKING SPEECH A CRIME

Governments in South Asia have approached the internet with a mindset of telecommunications regulation rather than respect for freedom of expression.

In India, the parliament is considering ways to reinstate the notorious Section 66A of the Information Technology Act which criminalised "offensive" matter on the net. This section was struck down by the Supreme Court of India in March 2015 with the court describing it as "open-ended and unconstitutionally vague". Adopted in 2009, Section 66A made it an offence punishable by up to three years' jail to publish electronically "any information that is grossly offensive or has menacing character." By making it a crime, enforcement of the amendment was in the hands of the police.

Among the offences pursued under this provision were:

- In 2011, cartoonist Aseem Trivedi saw his website cartoonistsagainstcorruption.com taken down on police order
- A school student was arrested for 14 days in Uttar Pradesh for a Facebook post critical of a state minister
- A complaint was lodged against Bangladeshi writer Taslima Nasreen for a tweet considered anti-Muslim
- An activist in Kerala was arrested for posting criticisms of Prime Minister Nrendra Modi on Facebook.
- Two schoolgirls in Mumbai were arrested – one for writing critically of the shutdown of Mumbai for the funeral of Shiv Sena leader Bal Thakeray and the second for liking the original post.

It was this final case that triggered the successful legal challenge by civil society groups against the law. In its ruling in March 2015, India's Supreme Court held that "sufficient definiteness (was) needed ...to define penal law". And this was clearly not the case with 66A, which tended to "arbitrarily, excessively and disproportionately invade the right of free speech and upset the balance between such rights and the reasonable restrictions that maybe imposed on such right". Reiterating a finding from an earlier case, the Supreme Court observed: "The law should not be used in a manner that has chilling effects on the freedom of speech and expression".

As a result of the decision, Google announced that it would cease take-downs at the request of the police or other executive authority, and would only implement take-down requests on the order of a court.

Despite the outcome, the government has indicated that it is examining ways to reinstate the intent of the law within the decision of the court. Police have continued to use the legislation against journalists. In March 2016, Prabhat Singh, a journalist for the Hindi daily *Patrika* from Dantewada district in Chhattisgarh, was arrested for posting allegedly obscene content on WhatsApp. This arrest was effected on a complaint registered by another journalist who happened to be on the same Whatsapp group. Prabhat Singh remains in the Jagdalpur jail where he is believed to have been beaten. Chhattisgarh has enacted a special security law to deal with a decade long Maoist insurgency and courts remain unwilling to grant bail when this law is invoked.

In Bangladesh, the publication by electronic means of anything likely to "prejudice the image of the State" or "hurt religious belief" is a crime under the Information and Communication Technology (ICT) (Amendment) Act, 2006.. Journalists and bloggers have been arrested and detained under the act and human rights organization Odhikar has been charged for publication of its report .

IFJ South Asia coordinator Ujjwal Acharya says: "The offense in the ICT Act is vague and unspecific. Under this section, anyone can be prosecuted for publishing material on a website or in digital form that is "fake and obscene," "creates the possibility for the deterioration of law and order," "prejudices the image of the State or a person" or which "may cause hurt to religious belief." Conviction can lead to between seven and 14 years imprisonment." Nearly 30 cases have been tried before a specially constituted cyber-crimes tribunal, and hundreds more are under investigation.

The proposed Cyber Security Act 2015 seeks to fortify the ICT Act, further tightening the power of the authorities to restrict alternative views.

In Pakistan, in April this year, the parliament adopted the Prevention of Electronic Crimes Bill, despite the widespread opposition of civil society groups. Rights group Boli Bhi's critique of the bill says that rather than simply addressing genuine cybercrimes, it criminalises acts which would be legal in an off-line environment.

The legislation has been criticised by UN Special Rapporteur on Freedom of Opinion and Expression, David Kaye, who said it could lead to censorship and self-censorship by the media. A joint statement by Bytesforall and related groups said the legislation empowered police and other authorities to enforce the law without adequate judicial oversight.

In the wake of the Indian experiences of Section 66A, the newly passed act in Pakistan provides a genuine threat to freedom of expression on-line.

In Nepal, journalists have also faced arrest for on-line news reports under clause 47 of the Electronic Transactions Act. This makes it an offence to publish online any material "which may be contrary to the public morality or decent behaviour or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities". Among the journalists affected have been those writing about business and politics.

SRI LANKA'S WAR ON (ONLINE) JOURNALISTS

Parallel to the long running civil war in Sri Lanka, was the war against the media. The front line of that media war, was often on-line.

The leading Tamil news website TamilNet, based in Europe, had early become the major source for war zone news missing from the Colombo media. This made it a target for the Rajapaksa regime and its supporters. In 2005, its editor Sivaram was abducted and murdered in Colombo. In 2007, as the war ramped up, the site was blocked by the Sri Lankan government.

Similarly, the first Sinhala news web site, Lanka-e-News, became a major target. Two days before the 2010 khaki elections called in the immediate aftermath of the end of the war, one of its online journalists and cartoonist, Prageeth Ekneligoda, was abducted by military operatives.

Following the election, the news website came under continuous threat. Its editor had to flee the country and on January 31, 2011, its Colombo office was burned down.

Many of the Sri Lankan journalists, who had to flee the country, launched news and opinion websites and face book pages from abroad. Lanka-e-news too moved to London. Between them, they became the new mainstream media for independent news about Sri Lanka. Even though many of these sites were officially blocked in Sri Lanka, the information they fed back into the country played a pivotal role in defeating the Rajapaksa autocracy in January 2015.



Credit: CC/Vikalpa

Under the Rajapaksa regime, journalists came under attack. Online websites were censored or shut down. The editor of one of the most critical websites, TamilNet, Sivaram was abducted and killed in 2005.

During that presidential election Lanka-e-news alone had nearly 2 million visitors a day. Perhaps that election can be claimed as the first in the world where independent on-line media fought back and changed the future of the country.

Sunanda Deshapriya

THE ATTACK ON BLOGGERS IN BANGLADESH

Credit: Suvra Kanti Das /AFP



A family photograph of Bangladeshi blogger Niloy Chakrabarti, who used the pen-name Niloy Neel, 40, with his wife is held up in their home in Dhaka on August 7, 2015. A gang armed with machetes hacked a secular blogger to death at his home in Dhaka August 7, 2015, sparking protests in the capital over the fourth such murder in Bangladesh this year.

Secular bloggers have been targeted by religious extremists in Bangladesh with the most recent, Xulhaz Mannan murdered in April 2016.

After protests from journalists and other activists, the government is finally taking some action to end the impunity in the attacks. Despite delays, arrests and prosecutions are starting.

On December 31, 2015, eight persons involved in the murder of blogger Rajib Haider were convicted and sentenced. Haidar had been hacked to death in February 2013 in Mirpur. The Dhaka Special Trial Tribunal sentenced to death Md Faisal Bin Nayem alias Dweep and absconding Redwanul Azad Rana. Rana was considered the mastermind of the murder while Nayeem attacked Haider with a meat cleaver.

Maksudul Hasan was given a life term sentence, two others were given 10-year jail terms and the chief of the militant group ABT Mufti Jashimuddin Rahmani was sentenced to five years while Sadman Yasir Mahmud was given three years.

In September 2015, five militants of the banned Ansarullah Bangla Team (ABT) were charged with the murder of Oyasiqur Rahman Babu in March 2015. Two were caught by locals immediately following the murder and handed over to the police. However, two others remain on the run and at large.

On August 29, Dhaka Police arrested Kausar Hossain Khan, 29, and Kamal Hossain Sardar, 29, for the murder of Niloy Neel, who was hacked to death in another 'machete murder' on August 7. The suspects are reported to be also members of the ABT. Two were arrested two weeks earlier for their suspected involvement.

On August 18, Bangladeshi police arrested Bangladeshi-Britisher, 58-year-old Touhidur Rahman, and two other suspects Sadek Ali and AminulMollick, for the killing of US Bangladeshi blogger and author Avijit Roy.

Most of them are currently awaiting trial in jail.

Yet, the attacks on bloggers continue.

DEFAMATION INTENSIFIES

At the same time as on-line media and other participants have been struggling with new laws criminalising content and restricting freedom of expression on-line, they have had to grapple with the application of traditional laws relating to defamation including criminal defamation.

Other than Sri Lanka and the Maldives, all south Asian countries have criminal defamation laws. Although they are not used as often as civil defamation they continue to have a chilling effect on freedom of expression. The Sri Lankan laws were abolished early this century if the wake of their widespread abuse by government officials. In 2004, the Human Rights Committee of the UN found that the use of criminal defamation in Sri Lanka violated the human rights of a journalist. The government subsequently repealed the laws.

In the Maldives, the Government is threatening to reintroduce the defamation law previously repealed in 2008.

The fight against criminal defamation suffered a major setback in May 2016 when the Indian Supreme Court rejected an application to find criminal defamation contrary to the free speech rights guaranteed in the Indian constitution. The court ruled that the constitution allowed certain restraints on freedom of expression, including the restraint of defamation.

In Bangladesh, prosecutors continue to use criminal defamation against journalists with charges laid by the government against two editors of prominent papers in February 2016.

Although the use of criminal defamation has been, justifiably, a focus of campaigning by press freedom organisations, the use of civil defamation has been as – if not more – damaging to freedom of expression in the on-line space.



Credit: Twitter/@AhmedSiddeeq

Journalists across the Maldives staged protests in 2016 against the government's proposal to recriminalize defamation. After the protests, a Maldivian government minister posted a photo to Twitter calling the journalists criminals.

Credit: Munir Uz Zaman/AFP



Since 2013, seven secular online bloggers have been hacked to death in Bangladesh. Protests have been held across the country calling on the government to guarantee freedom of expression.

In the wake of the Indian Supreme Court decision upholding criminal defamation, lawyer Bhairav Acharya wrote in the on-line publication The Wire (thewire.in): "Two kinds of defamation action have emerged to capture popular attention. First, political interests have adopted defamation law to settle scores and engage in performative posturing for their constituents. And, second, powerful entities such as large corporations have exploited weaknesses in defamation law to threaten, harass, and intimidate journalists and critics."

Acharya points out that this second use that has been most damaging for freedom of expression in the digital space. This is because both civil and criminal defamation complaints have been used to attack journalists and others publishing on-line through the use of Strategic Lawsuits against Public Participation, or SLAPP writs. In the on-line space these have effectively operated as take-down orders, often enforced by police.

Subramaniam Vincent, co-founder of the Bangalore-based web site citizenmatters.in, says the application of SLAPP writs is a major impediment to investigative reporting, particularly involving large corporations. The evidentiary bar required for a SLAPP writ is not high and most organisations find it easier to take-down the offending material or, simply to avoid investigating organisations known as litigious.

Although there has been an exciting growth in independent online voices in Indian media, few have the s resources that need to be dedicated to defending defamation actions which are often initiated just to get the work taken down. SLAPP writs are a major reason that on-line journalism has struggled to play the role it should in exposing corruption or empowering communities.

OPENING UP GOVERNMENTS

In most of South Asia, journalists working in the digital space are struggling to find the potential to truly hold governments and decision-makers accountable through transparency.

Over the past decade, parliaments in the region have started to adopt right to information laws which have helped open up decisions by governments and bureaucracies. In 2005, India adopted its Right to Information Act, followed by Bangladesh in 2009. Afghanistan adopted the Access to Information Act in November 2015. Legislation is currently before the parliament in Pakistan and in Sri Lanka, where it was a key plank in the 2015 presidential elections. There are

no laws in Bhutan (where recent legislation effectively failed in the legislature) or the Maldives.

Effective operation, however, requires proactive release of computerised access to information including malleable data. This is essential to empower journalists and activists to bring the tools of computational analysis to their work. The Indian act does require authorities to computerise records and follow certain transparency norms even in the absence of specific requests for information. The Bangladesh Act mandates proactive release, but does not require computerisation.

Effective use of the public and private release of data requires journalists and media organisations to embrace the opportunities offered by the power of computerisation to keep their communities informed and engaged.

South Asian media have participated in some of the major global exposures made possible by large scale document leaks. In 2011, *The Hindu* worked with Wikileaks to report on the Indian aspects of the cables leaks. Similarly, in Pakistan, *Dawn* published details of both the cable and Stratfor leaks. In 2016, journalists at the *Indian Express* worked as part of the International Consortium of Investigative Journalists on Indian citizens involved in the Panama Papers.

And despite the difficulties, on-line voices are emerging to take advantage of new models of data journalism. For example, in Bangalore, the website Citizenmatters.in is using data to track developments in the city and to challenge corruption. In Sri Lanka, Groundviews, published by the Centre for Policy Alternatives, uses data, for example, to track election violence and abuse.

SURVEILLANCE

Mass surveillance of telecommunications and on-line activities is widespread across south Asia. Often this surveillance is conducted through innocuous sounding organisations relying on over generous interpretations of legislative authority.

In India, the Centre for Development of Telematics (c-DOT)has been reported as implementing the benign sounding Lawful Intercept and Monitoring Project or the more Orwellian Central Monitoring System Project. At different levels, these projects intercept almost all types of internet communication both by working with ISPs and by interceptions without their cooperation or knowledge. The military run parallel surveillance.

Reporters without Borders has described C-DOT as one of the three worst on-line spies in the world.

In February 2016, the National Security Council Secretariat (NSCS) in India hinted that it was actively considering the establishment of a "media analytics centre" to track all social media postings. The explosive growth of social media and the security implications come up regularly at high-level conferences involving India's police and intelligence agencies. Though the political leadership has been known to caution that all modes of surveillance adopted should be consistent with fundamental rights guarantees, there has been very little public discussion of the implications for privacy and basic rights to free speech and information.

Pakistan has had its own system of data collection and monitoring. Telecommunications companies are required to hold communications data which can be accessed under warrant.

Credit: Munir Uz Zaman/AFP



Freedom of expression in Bangladesh has been under attack in recent years, with bloggers, journalists and activists threatened, intimidated and killed. Although the government has tried to address the issue, the actions have been insufficient in curbing the increased violence.

Credit: STRDEL/AFP



Indian Prime Minister, Narendra Modi ,is one of the world's most popular Twitter userswith millions of followers. Modi regularly uses social media to keep in touch with his supporters. However, during a visit to Kashmir in 2014, Modi had the internet shut down to prevent online discussions.

These warrants, however, are simple to obtain on grounds of having a "reason to believe" that a crime is being contemplated.

The country has also been a third party co-operator with the US National Security Agency and the related Five-Eyes organisations in mass surveillance of data, although there have been some reports that the British GCHQ has been undertaking surveillance in Pakistan on its own initiative. There have also been reports that, after the Snowden revelation in 2013 revealed the scope of technology available, the Pakistan authorities have sought assistance to build an equivalent national system.

Similarly in Bangladesh, the Government has budgeted Tk 150.51 crore (1,505.1 million Bangladeshi Taka) for a project to monitor online and social media activities. Under the project, a centre called the Cyber Threat Detection and Response Network will be set up.

In Sri Lanka, police and security have effectively unlimited authority under the Computer Crimes Act to access telecommunications data without warrant. The former Rajapakse government is believed to have implemented widespread surveillance technologies with the assistance of China. Both the previous President Chandrika Kumuratunga and the current President Maithrepala Sirisena have said they believed that the Rajapakse government was conducting mass surveillance, including surveillance of them and of other political opponents.

Journalists in South Asia need to work on the assumption that their telecommunications activity – including communications with otherwise confidential sources – is being intercepted and monitored by police. In regions of India such as Kashmir and Chhattisgarh, journalists have learnt to get accustomed to their phone calls being tapped.

ATTACKS ON JOURNALISTS

Apart from the legislative and regulatory restrictions, journalists, writers and campaigners in the digital space in South Asia have been targeted by religious and political extremists. This has been worst in Bangladesh where secular journalists and bloggers have been murdered and assaulted.

Despite the protests, this has continued with the latest being a journalist at an on-line gay rights publication, murdered in April. Xulhaz Mannan was stabbed to death, along with a companion, in his Dhaka home.

This was the latest in a series of attacks which are stifling free expression in the country. Mannan's murder followed six killings of people who were writing or publishing secular blogs on-line. Religious extremists, including groups claiming affiliation with Al-Qaeda, have boasted of their role in the killings. The ruling authorities have discounted these claims and insisted that the crimes have been committed by local groups. Their response has also elicited some public disquiet for being disturbingly like a form of blaming the victim.

In Pakistan – now one of the most dangerous places for journalists in the world – journalists working in the on-line space have been murdered or attacked for their reporting.



Sabeen Mahmud was brutally murdered in Karachi on April 25, 2015. The outspoken activist's murder was widely condemned on social media. Worryingly, many her condemned the murder on social media were later threatened.

Credit: Facebook

In May 2015, prominent human rights activist Sabeen Mahmud was killed shortly after hosting an event on Balochistan's 'disappeared people' on April 25, 2015, in Karachi. She was an outspoken human rights advocate and the director of T2F (The Second Floor), a café and arts space that has been a mainstay of Karachi's activists since 2007.

In August 2015, a freelance journalist, Zeenat Shahzadi, who distributed much of her work through Facebook and Twitter was kidnapped in Lahore. She is believed to have been taken by the security service because of her campaigning journalism over an Indian citizen missing in Pakistan. She remains untraced at the time of writing, amid rising fears about her safety.

In India, journalist Jagendra Singh was burnt to death in June 2015. His dying declaration held a minister in the northern Indian state of Uttar Pradesh responsible, allegedly in retaliation for some critical Facebook posts.

These experiences suggest that in south Asia, those who attack journalists increasingly focus on writers and journalists working in the digital space. As the internet becomes more widespread, on-line publications attract greater attention, including from those who wish to censor through murder. In the face of these attacks, there has been some criticism from on-line activists that traditional journalists and their organisations are slower to respond to attacks in the digital space.

Within the internet and online media itself, there is evidence of increasing trolling and harassment of journalists with women journalists bearing the brunt with reports indicating that women and three times as likely to be abused on-line as men. As the IFJ's 2016 South Asia report on press freedom says: "while the internet and online media does provide a more democratic platform for interaction and sharing of a plethora of news and views, the 'dark matter' of the internet also perpetuates all the discrimination and invisibility that women have experienced from traditional media. While it mirrors and magnifies the discrimination faced by women in society."

The report reveals the impact of abuse or online harassment can be devastating as more and more peoples' communication is mediated in an online world.

Three categories of attacks directed at women on the internet have been identified:

- personal attacks that target women with threats of rape, killing or 'doxing' (publishing personal information, which encourages further attacks);
- campaigns to demean women as a group (calling them 'feminazis', for instance); and
- reflexive misogyny where people talk in a misogynistic way whether they intend it or not.

In south Asia, many of these attacks are dressed up with religious or nationalist rhetoric. So severe are these attacks in Bangladesh that the IFJ reported that female journalists and bloggers who attended an IFJ workshop on gender equity in Dhaka in November 2015 said that they usually blog under aliases. However, they said, this does not prevent them from getting threats of sexual violence, rape and mutilation.

Assertion of women's rights, no matter how gently expressed, brings a deluge of attacks in response. For example, the participants at the IFJ workshop said that criticising the religious diktat prohibiting women from attending college unless they are veiled, provokes a barrage of misogynistic threats.

In Pakistan, it appears there is at least some institutional support for the attacks on women. The *Dawn* newspaper reported that a Facebook page called ISI (the acronym for the leading military security service) hosts photographs of prominent human rights activists, many of them women, encouraging their followers to rape and murder them. The page has over 34,000 followers. While the military has dissociated itself from these pages, human rights activists believe that pages such as these would not exist without covert state support.

Throughout the region, women are pushing back against misogynist trolling. In India, for example, women journalists combine on-line to respond to attacks on individuals. At times it seems this can makes things worse. For example, the killing of Sabeen Mahmud sparked grief, anger and condemnation on social media in Pakistan. The IFJ reports that barely a week later, there were dangerous threats and calls for attacks on those who tweeted or expressed support for her, prompting many of those targeted to go offline.

Amendments to the Indian penal code introduced in 2013 after the brutal gang-rape of a young woman in Delhi caused nation-wide outrage, defines the offence of "stalking" as monitoring "the use by a woman of the internet, email or any other form of electronic communication"; and watching or spying on "a woman in any manner, that results in a fear of violence or serious alarm or distress in the mind of such woman, or interferes with the mental peace of the woman". Trolling, or verbally abusing a woman on social media and through email is curiously left out of this definition of offences. Certain high profile police complaints though have been lodged recently over the harassment that particular journalists have been subject to on Twitter and Facebook.

Men are not exempt from religious or national attacks on line. As one on-line journalist said: "Mention something like Kashmir and watch the thousands of attacks roll in."

Seniority is not protection. In April, prominent cricket writer Harsha Bogle was removed from covering the Indian Premier League after he was attacked on Twitter (including by Amitabh Bachchan and MS Dhoni) for being insufficiently nationalist in commentating on Indian cricketers in the competition.

CONCLUSION

The digital space in South Asia is at a pivot point. As the Internet becomes near universal through mobile, journalists and freedom of expression activists need to grasp the opening it offers to entrench principles of free expression, open access and limits on surveillance into the architecture and practice of the web in the region.

This means journalist organisations need to properly integrate freedom of expression in the digital space in its human rights work. They also need to reach out and work with digital activists to ensure the internet in South Asia can deliver on its promise of open communication that informs and entertains the diverse communities of the region.



Credit: Munir Uz Zaman

As the internet becomes a universal tool for journalists and freedom of expression activists, new challenges and threats are arising which ultimately create new dangers for those telling important stories from the region.