The Internet and State Intervention in Asia:
A Comparative Study of Selected Countries

In context of contemporary debates about censorship, net neutrality and the role of the state in today's globalising world, it becomes vital to examine the stand taken by various Asian governments towards a free and uncensored internet. This report presents a comparison of twelve Asian countries: Bangladesh, China, India, Indonesia, Japan, Myanmar, Nepal, North Korea, Pakistan, South Korea and Sri Lanka, and briefly explores the role of these governments in cyberspace.

Nandini Bhattacharya[1], **Rituparna Dutta**[2], **Radhika Chakraborty**[3] **and Aakriti Singh**[4]

eSocialSciences

This report draws from secondary data on the state of the internet in Asian countries. Using a fixed set of indicators, the report compares twelve countries on the basis of internet penetration, recent legislation, regulatory bodies and state control over telecom providers; and presents a brief summary of the degrees and means of state control over the internet as well as recent incidents of cyber censorship. The intention was to make ready data on the internet in Asian countries accessible and concise, and enable a comparison of the extent of state intervention.

[1] nandini.sen.bhattacharya@gmail.com
[2] rituparna.dutta@esocialsciences.com
[3] radhika.chakraborty@esocialsciences.com
[4] aakritisingh31@gmail.com

Bangladesh

Internet Penetration: 6.50 per cent

Recent Legislation: National Information and Communication Technology Policy, 2015

Regulatory Bodies: Bangladesh Telecommunication Regulatory Commission

Telecom Providers: Bangladesh T&T Board is the largest state owned internet service provider in Bangladesh. It was established by the government in 1979.

There is very little, or no evidence of internet filtering found by internet investigative collective OpenNet Initiative in 2011. Although Internet access in Bangladesh is not controlled by a national level filtering regime, the state has interceded to block websites for hosting anti-Islamic content and content considered rebellious.

In 15 July 2008, the Bangla blogging platform Sachalayatan migrated to a new IP address after being reported inaccessible. It was likely the first filtering incident in Bangladesh, although it was not officially confirmed. In another event when a doubtful video was uploaded in YouTube covering a partial audio record of a meeting between the prime minister and military officials, YouTube was blocked for a few days in March 2009 in order to protect 'national interests'.

The Bangladesh Telecommunication Regulatory Commission (BTRC) blocked Facebook for seven days in 2010 because of images portraying the Islamic prophet Mohammad and several of the country's political officials as well as links to pornographic sites. The block was withdrawn after Facebook agreed to remove the offensive content. In the capital city of Bangladesh, during the same time, a person was condemned of uploading satiric pictures of some political leaders on Facebook.

In September 2012, YouTube was again blocked by the BTRC after the controversial film, *Innocence of Muslims,* was not removed from the site.

China

Internet Penetration: 47.4 per cent

Recent Legislation: In 2001, Human Rights Watch estimated that over 60 sets of government internet regulations have been issued by the Chinese government, and many new regulations have been issued since then. These national regulations are supplemented a number of provincial and local-level implementing regulations, guidelines, policy documents, and other legal instruments. Measures on the Administration of Internet Information Services (2000), Provisions on the Administration of Internet News and Information Services (2005), Regulations on the Administration of Internet-Based Audio-Visual Program Services (2007), are some of the more important pieces of legislation regarding internet censorship.

Regulatory Bodies: Ministry of Information Industry (MII). Policy about what substantive content is to be censored is largely directed by the State Council Information Office and the Chinese Communist Party's Propaganda Department, with input from several other government and public security organs.

Telecom Providers: There are nine state-licensed Internet Access Providers (IAP), all of which have foreign connections. The individual Chinese Internet user buys Internet access from one of several thousand Internet Service Providers (ISPs), who are in effect retail sellers of Internet access that is in turn purchased wholesale from the nine IAPs.

Human Rights Watch estimates that today approximately 12 different government ministries have some degree of authority over the Internet. The first level of internet censorship is in the form of filtering of content at the router level, which is configured into the hardware of the internet in China. The next level of censorship comes in the form of making ISPs liable for the content they host, and the third is through making Internet Content Providers legally liable for the content posted on their websites irrespective of who posts it. This encourages self-censorship and breeds a culture of fear and surveillance; a vital strategy for the censors in light of the vast population of internet users in China. (Human Rights Watch, 2006)

Amnesty International in 2008 reported that China has employed between 30,000 and 50,000 special Internet police who, with the aid of Western-provided technology, monitor individuals' emails, conduct surveillance, and check for banned websites and content; and in 2013 BBC News suggested that over two million microblog content monitors are employed by the Chinese state. Amnesty said, 'On screen, Internet users looking at China's most popular websites will see a cartoon cyber-police officer appear every half hour. The cartoon officer reminds them not to view censored material' (Amnesty International, 2008). The so-called 'Great Firewall of China' prevents users in China from accessing international sites such as Facebook, Twitter and YouTube, and the state is backing state-friendly clones of these sites. (Wines, Franiere and Ansfield, 2010)

China has recently launched what is being called the 'Great Canon'. Unlike the firewall, this new weapon is meant for the offensive, and allows Chinese officials to launch attacks against sites across the world they deem hostile; taking their censorship past their own national borders. (Perlroth, 2015). The Diplomat reported that recently, GitHub and its page GitFire, a site dedicated to tracking and exposing Chinese censorship, were the targets for a massive distributed denial of service (DDoS) attack. (Tiezzi, 2015) China also recently banned online medical diagnosis (Dasgupta, 2015), is prosecuting several video portals for hosting violent Japanese anime (Bischoff, 2015), and has periodically blocked amongst others, Reuters News, BBC, Youtube, Facebook, Google. Twitter, Hotmail and Amazon.

Table 1: Internet Penetration in Asia (Selected Countries)

Table 1 - Internet Users (per 100 people)																		
Data Source																		
Country Name	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
India	0.5275324	0.6601464	1.5578756	1.68649	1.9761365	2.3880735	2.8054999	3.95	4.38	5.12	7.5	10.07	12.580061	15.1
Pakistan		1.3185508	2.5774267	5.0411581	6.164321	6.3323291	6.5	6.8	7	7.5	8	9	9.96	10.9
Japan	29.99074	38.532061	46.594201	48.452366	62.39393	66.9210666	68.68527	74.3	75.4	78	78.21	79.054114	86.25	86.25
Thailand	3.6890413	5.5563261	7.5312303	9.2990272	10.677303	15.026004	17.160715	20.03	18.2	20.1	22.4	23.669926	26.46	28.94
Myanmar		0.0002893	0.0004265	0.0240641	0.0243574	0.0652389	0.1820483	0.2171284	0.22	0.22	0.25	0.98	1.0691	1.2
China	1.7759152	2.6396502	4.5957043	6.2	7.3	8.532257	10.522153	16	22.6	28.9	34.3	38.3	42.300117	45.8
Bangladesh	0.0710394	0.1298008	0.1399203	0.1638777	0.1990363	0.2416373	1	1.8	2.5	3.1	3.7	5	5.75	6.5
Korea, Rep.	44.7	56.6	59.4	65.5	72.7	73.5	78.1	78.8	81	81.6	83.7	83.75912	84.073226	84.77
Indonesia	0.9255639	2.0186139	2.1941357	2.3870198	2.6002859	3.6020248	4.7648131	5.7862747	7.9174794	6.92	10.92	11.11	14.7	15.82
Nepal	0.2046517	0.2400153	0.3129561	0.3828109	0.4498437	0.8265513	1.1413892	1.41	1.73	1.97	7.93	9	11.1495	13.3
World	6.7703695	8.0958589	10.586327	12.285252	14.182289	15.799655	17.618863	20.553266	23.273446	25.947307	29.347107	32.018793	35.581119	38.132338855
*Source - World Development Indicators														

India

Internet Penetration: 19.19 per cent

Recent Legislation: Indian Telegraph Act 1885; Indian Wireless Telegraphy Act 1933; Information Technology Act (IT) 2000 and the Indian Penal Code, 1860 (IPC)

Regulatory Bodies: Telephone Regulatory Authority of India (TRAI)

Telecom Providers: Bharat Sanchar Nigam Limited and Mahanagar Telecom Nigam Limited are state owned internet service providers. Aside from these two public sector companies, the TRAI lists over 172 private internet service providers. Of these, major players include telecom operators like Airtel, Reliance Communication, Tata DoComo, Tata Indicom, Vodafone, Airtel among others.

The dawn of the twenty-first century has seen online and media censorship in India to an unprecedented degree. According to Freedom House, an independent think tank, India's freedom of speech online and in the media is partially fettered by the laws in the country. While religious and political content has traditionally been off limits to all but a few chosen media persons/politicians, of late social issues have come under fire of the moral brigade as well.

News channels, social media websites and search portals are usually blocked by the authorities in the face of communal violence or religious sensitivity. For instance, over 80 websites were blocked during and after the Muzaffarnagar (Uttar Pradesh) riots, a horrific incident which resulted in immense mortalities and wide scale dislocation of religious minorities in the state. In a similar case, as religious groups protested the movie *Innocence of Muslims* (2012), social media websites were partially blocked in order to avoid an escalation of violence. It is not rare for websites to be blocked in the North-Eastern states of the country.

Sections 69-A of the Information Technology Act, and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 are legislations that allow for the state to issue diktats regarding cyber censorship. The Blocking Rules apply to orders issued by government agencies, who must appoint a 'nodal officer' who sends the requests to the 'designated officer,' and demonstrate that they are necessary or expedient under Section 69-A.The designated officer chairs a committee which includes senior representatives of the law, home affairs, and information ministries, and the nodal agency for cyber security, the Indian Computer Emergency Response Team (CERT-IN). Indian courts can order content blocks without this review process. The government asked social networking sites to block 1,299 URLs in compliance with court orders between January 2013 and January 31, 2014, compared to 8, 21, and 352 URLs in 2010, 2011 and 2012, respectively.

Until recently, individuals could be prosecuted for libelous or defamatory statements or ideas published online, under Section 66-A of the Information Technology Act 2009. In 2012 two young women were arrested under the act over a Facebook post criticising the shutdown of Mumbai after the death of a local hardline politician. One was arrested for 'liking' the post. In the same year, a university professor in West Bengal was detained for sharing a political cartoon. These are not isolated cases. Prominent journalists are now harassed politically over the act of criticising politicians or events using Twitter.

After a spate of terror attacks in the country, the central government utilised the Central Monitoring System (CMS) in 2014, a clandestine mass electronic surveillance data mining program which gives law enforcement agencies centralised access to India's telecommunications network and the ability to listen in on and record mobile, landline and satellite calls and voice over Internet Protocol(VoIP), and read private emails, SMS and MMS and geolocate people via their cell phones all in real time.

To date, incidents of online censorship have been highlighted by the media in 2015. In February 2015, the Indian Government blocked screenings of the BBC documentary *India's Daughter* in public theatres, and ordered Youtube to make it unavailable for viewers in the country. Recordings of a 'comedy roast' , a type of live performance by a group of comedians came under intense scrutiny, and was ordered to be blocked on Youtube, Facebook, Twitter and other news/social networking sites. A massive campaign has been hoisted by internet activists in the country in order to prevent TRAI from adopting discriminatory policies with regards to over-the-top services.

The journalism collective Reporters without Borders (RWB) put India on its list 'countries under surveillance' in 2012, citing the state's increased surveillance, which essentially translated to a fundamental breach of the Indian citizens' privacy. Following the string of controversies that have dogged the cyberspace in India, RWB has placed India in its list of *Current Enemies of the Internet*.

Indonesia

Internet Penetration: 28.1 per cent

Recent Legislation: Law on Information and Electronic Transactions (2008)

Regulatory Bodies: Ministry of Communications and Information Technology (MCI)

Telecom Providers: Telkom is the main player in providing internet services in Indonesia. It is a semi-privatised, majority state-owned company.

According to the OpenNet Initiative in 2011 grounded on testing done during 2009 and 2010 internet filtering in Indonesia was recorded as generous in the social area and as discerning in the political and Internet tools areas. There was no indication of filtering in the conflict/security area. Indonesia was graded 'partly free' in Freedom on the Net 2011 with a score of 46, midway between the end of the 'free' range at 30 and the start of the 'not free' range at 60.

The discerning blocking of websites started in 2007–2008. YouTube was blocked in April 2008 by the ISPs after Google not responding the government's request to remove the film *Fitna*, by the Dutch parliamentarian Geert Wilders, which supposedly mocked the Islamic prophet, Muhammad. Again in May 2010, government officials sent a letter to Facebook commending closure of an account which promoted a competition to draw Muhammad. It also asked all ISPs to limit access to the account's link.

The Law on Information and Electronic Transactions (ITE Law) was passed by the government in march 2008, under which a person can be condemned up to six years in prison and a fine of up to 1 billion rupiah (US$111,000) if found committing defamation online. Until June 2010, at least eight citizens were condemned under this law for defamation charges for comments on e-mail lists, blogs, or Facebook.

In 2012, one of the ISP used Internet censorship policies to prevent users from accessing Google-related websites. In 2014, government alleged several sites for hosting content that includes nudity and censored them. This includes Vimeo, Reddit, and Imgur.

Japan

Internet Penetration: 86.03 per cent

Recent Legislation: Provider Liability Limitation Act 2001; the Law Concerning Nippon Telegraph and Telephone Corporation, Etc. 1999

Regulatory Bodies: Is characterised by self-regulation. The Ministry of Internal Affairs and Communications (MIC) oversees the telecommunications, Internet, and broadcast sectors.

Telecom Providers: Unlike many other countries, internet service is provided into two parts - usually by different companies, and both services are required to be connected to the internet. Internet Carrier Services provide the actual connection, such as ADSL or fibre optic. Internet Service Providers, provide the User ID and Password as well as technical support. Some companies such as SoftBank provide both Carrier and ISP services. Most ISPs, however, work in association with the Nippon Telegraph and Telephone Corporation East and West divisions. KDDI Corporation and some other companies also provide these services, often because they lease the line from NTT East or NTT West.

Internet services were introduced by the Nippon Telephone and Telegraph Corporation (NTT) in association with Fujitsu in 1996. Internet penetration in Japanese households is about 86 per cent, the figure rising to about ninety per cent for business and industry usage. Till date, NTT has almost a monopolistic control in the industry, and provides last mile coverage, even for competing Internet Service Providers (ISP). There are no state internet regulators as service providers favour self-regulation.

Article 21 of the Japanese Constitution prevents censorship laws being put into place, however, the state utilises Article 175 to carry out their censorship agenda. In general, however, the Japanese establishment is considered liberal.

In 2008, the Japanese government briefly considered regulating the internet for libelous content from 2010 onwards in a study titled *Final Report on a Comprehensive Legal System for Communications and Broadcasting*. This proposal was never carried out due widespread media outrage at the time. The government did prosecute the publishers of a manga (Japanese comic) for the obscenity in 2004 (although public opinion considered this move justified), and finally criminalised child pornography in 2006. Political speech was constrained online for 12 days before the December 2012 election under a law banning parties from campaigning online.

Myanmar

Internet Penetration: 1.2 per cent

Recent Legislation: Myanmar Draft Telecommunications Law (2012), Electronic Transactions Law (2004), Printers and Publishers Registration Act (1962), Electronic Transactions Law (2004).

Regulatory Bodies: Censorship and Registration Division

Telecom Providers: Two major operators are Myanmar Posts and Telecommunications (MPT) and Yatanarpon Teleport

Though Myanmar has a population of over 53 million, the fixed telephone subscription rate, mobile cellular subscription rate and internet penetration rates of Myanmar are 1.26 per cent, 1.24 per cent and 0.2 per cent respectively. (Herber Smith 2012) In 2013, telecom providers were expanded to include international providers. Though ISPs were still largely state-run as of 2014, they seem poised for privatisation.

Freedom House reports that media censorship was officially abolished in 2012, and the situation improved in 2013. However, despite the official lifting of censorship, the state still exerts coercive pressure on explicitly political content. The state maintains the capability to conduct surveillance of communication methods. Though internet and telecommunication technology is becoming more accessible, there is still a vast nexus of military control and power. Added to this is the fact that despite legal reform, the new Telecommunications Law of 2013 did not abolish the previous regime of harsh punishments for political dissent expressed on the internet. Freedom House reports that Zaw Pe, a digital video journalist was sentenced to a year in prison in relation to an interview he conducted in 2012. (2014) Though internet activists who had previously been imprisoned under the military regime have been released since 2011, this was done under the terms of amnesty and on the condition that they would not repeat their offences. The current Constitution of Myanmar does not guarantee freedom online. Freedom House writes that the new Telecommunications Law permits government agencies 'to direct the organisation concerned as necessary to intercept, irrespective of the means of communication, any information that affects the national security or rule of law.' (2014)

Nepal

Internet Penetration: 13.3 per cent

Recent Legislation: Electronic Transaction Act 2006

Regulatory Bodies: Nepal Telecommunication Authority

Telecom Providers: Nepal Telecom, the state-owned company is leading the market with nearly 58 per cent market share.

In Nepal, the OpenNet Initiative steered a testing on six ISP, (Worldlink, Everest, Mercantile, Nepal Telecom, Speedcast, and Websurfer) from October 2006 through January 2007 to identify possible Internet censorship.

The tests showed no evidence of filtering. The Nepali constitution guarantees enumerated liberty to publish on the Internet.

However, according to the Electronic Transaction Act 2006, ISPs should limit storing, disseminating, broadcasting websites having pornography, horror and extreme violence. Following a request from the Home Ministry, Nepal Telecommunications Authority (NTA) has been working with ISPs and telecom operators to ban sites that have pornographic content.

North Korea

Internet Penetration: ?

Recent Legislation: ?

Regulatory Bodies: ?

Telecom Providers: The only ISP in North Korea is the state-run Star Joint Venture Co. that uses a fibre-optic cable that runs between Pyongyang and Dandong in China. There is also a satellite link to Germany that is occasionally used to bolster the connection.

The North Korean state's mass surveillance extends to the internet as well. Internet usage is tightly controlled by the government. The internet is inaccessible to most of Korea's population, and uncensored cyberspace is visible only to a small group of privileged individuals: high level government officials, propagandists and media workers, and state officials, researchers and hackers. (Kim and Lee, 2014) It is likely that the government monitors this access as well. Kwangmyong or 'bright star' is North Korea's intranet, which is accessible to a slightly larger net of people. This enables access to approximately 5,000 websites, which have been filtered by the state-controlled Korea Computer Center. (Sedaghat, 2014) However, owning a computer requires permission from the government, and all personal computers are registered with the police.

Despite preventing most of its population from accessing the internet, the North Korean state harnesses the internet for propaganda and cyber warfare. Vox reports that a group of trained hackers in North Korea are used to launch high profile cyber warfare attacks (Fisher, 2014). From 2011 onwards, these hackers have been targeting South Korean banking systems, and computer systems of television broadcasters. (Fisher, 2015) North Korea's internet was in the news most recently regarding the controversial Sony Film *The Interview*, which depicted Kim Jong Un in what the North Korean state deemed to be an unflattering light. Sony was cyber-attacked, and the United States government accused North Korea to the hacking (Sanger 2015). Later in the year, the entire North Korean internet system was brought down, in what many suggested was an act of retaliation (Frizell, 2014). These attacks are used as a display of state power and aggression.

Foreigners in the can use 3G connections on their mobile devices to access the internet, but citizens are restricted from doing so. (Sparkes, 2014). Korea recently has banned foreigners from accessing Twitter and Facebook. In 2013, Korea cracked down on foreign embassies' and foreigners' Wi-Fi connections, which were reportedly unsecured and were thus being accessed by locals. (Keck, 2014)

Pakistan

Internet Penetration: 10.84 per cent

Recent Legislation: Pakistan Telecommunication (Re-Organisation) Act, 1996 (with 2006 amendments), National IT Policy and Action Plan (2000)

Regulatory Bodies: Pakistan Telecommunications Authority, Ministry of Information Technology, Pakistan Electronic Media Regulatory Authority

Telecom Providers: In 2012, the Internet Service Providers Association of Pakistan had over 50 registered members which provided a variety of options such direct subscriber line, broadband cable services, fibre to home services and domestic fibre backbone. Pakistan Telecommunication Company Limited (PTCL) is the backbone of the telecommunications infrastructure in the country. PTCL was originally a public sector company. In a bid to privatise the company, the government sold a major percentage of the shares of the company in 2006. Other major players in this industry include Wateen, Worldcall Telecom among others.

Pakistan is considered to have some of the world's strictest laws regarding blasphemous material. The 1973 Constitution of Pakistan considers Islamic rules and principles as fundamental elements to guide the development of law in the country. Article 227 specifically obliges the state to develop laws in accordance with Islamic teachings and restricts the development of any law that is not as per the teachings of Quran and Sunnah. Thus, most aspects of governance are filtered through a religious prism. Due to the religious nature of state policies, and legislation, Pakistan has a chequered history of internet censorship. In 1986 the Penal Code of 1860 was amended by the military regime of General Zia-ul-Haq. The amended laws prescribed life imprisonment or death for certain violations. Religious minorities and separationist groups (like Balochi, Sindhi, Ahmadi) have been systematically blocked from the Pakistani cyberspace.

In 2012, National ICT R&D Fund, a division of the Ministry of Information Technology, proposed to run a massive filter- 'National URL blocking and filtering system' which would block up to 50 million websites, with a delay of not more than 1 millisecond. The idea for this filter was based on close South Asian neighbor China, which has successfully run the Golden Shield or Great Firewall, responsible for blocking websites from around the world. The Pakistan Telecommunication Authority has already blocked 13,000 websites considered guilty of publishing adult and blasphemous content.

One of the largest instances of blocking websites occurred in the international uproar over the depiction of the Islamic Prophet by Danish newspaper Jyllands-Posten on 30 September 2005. A blanket ban was imposed on blogging platforms like blogspot.com, which was not revoked until late 2006, over a year later. Since 2010, Pakistan has regularly blocked Youtube, Facebook and blogging tools like blogger.com, along with 450 other news and social media sites. Google Inc. owned Youtube has been sporadically blocked since 2008 until 2014, as regulators found too much un-Islamic content on Youtube, such as the parts of the 2012 movie *Innocence of Muslims*.

South Korea

Internet Penetration: 92.4 per cent

Recent Legislation: Internet Content Filtering Ordinance (2001), Telecommunications Business Act (1991), amended Telecommunications Business Act (1995). In June 2002, the Supreme Court struck down the provisions of the Telecommunications Business Act defining 'harmful' content and granted the government unlimited authority to regulate harmful Internet content. Also relevant is the Act on Promotion of Information and Communications Network Utilisation and Information Protection (Information Act) (2007).

Regulatory Bodies: In February 2008, the Korea Communications Commission (KCC) was created to consolidate the MIC and the Korean Broadcasting Commission (KBC). The regulation of Internet content is conducted by the Korean Communications Standards Commission (KCSC; formerly KISCOM) and the National Election Commission (NEC).

Telecom Providers: There are three major telecom providers in South Korea: SK Telecom, KT and LG UT. There are six internet providers as of 2002, the largest of which is KT.

Though South Korea's internet is said to rank amongst the fastest in the world and internet penetration stands at over 90 per cent, Freedom House classifies South Korean internet as only 'partly free' and claims free expression has been diminishing since 2008. (Freedom House, 2014) OpenNet suggests that South Korea's fraught relationship with North Korea is a sensitive domain for censorship, and the government's strong stand against communism leads to a high level of political policing. (OpenNet, 2012) Electronic Frontiers Australia (EFA) reports that as of 2001, the government had mandated the blocking of over 120,000 sites that contained words in a control list of keywords. The Economist reports that in the last year approximately 23,000 South Korean web pages were deleted, and 63,000 more were blocked. (2014)

In 2011, criticism of South Korea's censorship policy emerged from within the KCSC—one of its members posted samples from censored content on his blog and opened these up for deliberation, and controversy erupted over his indictment in 2012. (Freedom House, 2012) In December 2013, police accessed private social network accounts and real time location information regarding the interrogation of leaders of a railway union protest. (Freedom House, 2014)

The New York Times reported earlier this year that the country's three main telecommunication companies have been funneling user data to law enforcement agencies without a warrant, or even informing users. In 2012, the National Intelligence Service was accused of monitoring and participating in Internet discussions about the election campaign to influence users in favour of Park Chung-hee and discredit the opposition. In October, it was revealed that the N.I.S. had surveilling chats on KakaoTalk, the most popular mobile messaging app, to uncover apparently pro-North Korea activists. (Koo, 2015) Many other such instances of surveillance, and in particular the stringent monitoring and censoring of North Korean sites and pro-North Korean voices, has been a cause for major criticism of the South Korean state's role.

Sri Lanka

Internet Penetration: 21.9 per cent

Recent Legislation: Sri Lanka Telecommunications Act (1991)

Regulatory Bodies: Telecommunications Regulatory Commission of Sri Lanka (1991)

Telecom Providers: There are many service providers in Sri Lanka, amongst which are Eureka, hutch, LankaCom, Mobitel (Sri Lanka Telecom)

Human Rights Watch said that 'Government-enforced codes of conduct on the media invariably infringe upon the right to free expression as established under the International Covenant on Civil and Political Rights'. (2013) Beginning in 2006, the then Sri Lankan government began a policy of blocking pro Liberation Tigers of Tamil Eelam (LTTE) websites. Websites such Tamil Net, Tamil Canadian, LankaNet, Nidahasa, among others were blocked until well after the war ended, in 2010. Certain independent news website like LankaeNews, LankaNewsWeb, InfoLanka and Sri Lanka Guardian were blocked in January 2010 a few hours before the presidential election results were announced.

Human Rights Watch reported that in 2013, the Ministry of Mass Media and Information officially proposed a Code of Media Ethics that would apply to print and electronic media, including the Internet. This code contained 13 types of substantive speech that would be prohibited from publication, including content that vaguely 'offends against expectations of the public, morality of the country, or tend to lower the standards of public taste and morality.' The code also restricts content that 'contains criticism affecting foreign relations,' which could lead to sanctions for reporting on international criticism of Sri Lankan government actions.

Thailand

Internet Penetration: 29.7 per cent

Recent Legislation: The Electronic Transactions Act 2001

Regulatory Bodies: Ministry of Information and Communications Technology (MICT), including the National Information Technology Committee and National Electronics and Computer Technology Centre

Telecom Providers: There are currently three major private mobile carriers; Advanced Info Service (AIS), Total Access Communication Public Company Limited, commonly known as DTAC, True Move. The state-owned ISP is Telephone Organization of Thailand (TOT).

In the Freedom House rankings, Thailand moved from Partly Free to Not Free. Freedom House reports that court rulings in Thailand decreed that the lèse-majesté law did not contradict constitutional provisions for freedom of expression, and made third-party hosts liable for lèse-majesté content posted online. (Freedom House 2013). Internet censorship is conducted by the Royal Thai Police, the Communications Authority of Thailand, and the Ministry of Information and Communication Technology (MICT). With the enactment of a new cybercrimes law in June 2007 (Act on Computer Crime B.E. 2550), Thailand became one of the few states in Asia whose government was required to obtain court authorisation to block Internet content.

Freedom House reported that 'online censorship intensified after April 7, 2010, when the government declared a state of emergency and created a mechanism allowing the authorities to suddenly block without a court order any website considered to be publishing politically sensitive or controversial information' (2013). These websites included specific YouTube videos, Facebook groups, and Google groups. International news websites and human rights groups also remained accessible.

Conclusion

The openness of the Internet attributes its success. As such, maintaining the open and free character of the global Internet within the country is the responsibility of the government. Ensuring open access to the Internet, warranting internet freedom, and securing the rule of law online is the central and crucial role of the state. Given the borderless, global nature of the internet, along with the responsibilities of the state, internet governance is also a very important global issue. As a result, internet freedom is both a national and international policy subject.

References

Bangladesh

Heacock, Rebekah. (2010). Pakistan Lifts Facebook Ban; Bangladesh Cracks Down. *OpenNet Initiative.* Available at https://opennet.net/blog/2010/06/pakistan-lifts-facebook-ban-bangladesh-cracks-down

BBC News. (2010, May 30). Bangladesh 'blocks Facebook' over political cartoons. *BBC News.* Available at http://www.bbc.com/news/10192755

BBC News. (2010, June 6). Bangladesh unblocks Facebook after Muhammad row. *BBC News.* Available at http://www.bbc.com/news/10247858

Table 1 - World Bank Data Sets
Available at http://data.worldbank.org/indicator/IT.NET.USER.P2

China

For more details on legislation regarding internet regulation, please visit http://www.hrichina.org/en/content/3244

For more statistics on blocked websites in China, please visit https://en.greatfire.org/

Amnesty International. (2008, March 28). What is internet censorship? *Amnesty International*. Available at http://www.amnesty.org.au/china/comments/10926/

BBC News. (2013, October 4). China employs two million microblog monitors state media say. *BBC News.*

Available at http://www.bbc.com/news/world-asia-china-24396957

Bischoff, Paul. (2015, April 1). China's top video sites to be punished over violent Japanese anime. *TechinAsia.* Available at https://www.techinasia.com/chinas-top-video-sites-punished-violent-japanese-anime/

Human Rights Watch. (2006). How Censorship Works in China: A Brief Overview.*' Race to the Bottom' Corporate Complicity in Chinese Internet Censorship.* Available at http://www.hrw.org/reports/2006/china0806/3.htm

MacKinnon, Rebecca. (2009, June 2). China Blocks Twitter, Flickr, Bing, Hotmail, Windows Live, etc. Ahead of Tiananmen 20th Anniversary. *CircleID*.
Available at http://www.circleid.com/posts/20090602_china_blocks_twitter_flickr_bing_hotmail_windows_live/

McKirdy, Euan. (2015, February 4). China's online users more than double entire U.S. population. *CNN*. Available at http://edition.cnn.com/2015/02/03/world/china-internet-growth-2014/

Perlroth, Nicole. (2015, April 10). China Is Said to Use Powerful New Weapon to Censor Internet. *The New York Times*. Available at http://www.nytimes.com/2015/04/11/technology/china-is-said-to-use-powerful-new-weapon-to-censor-internet.html

Tiezzi, Shannon. (2015, April 3). Has China Weaponized the Internet? *The Diplomat*.
Available at http://thediplomat.com/2015/04/has-china-weaponized-the-internet/

Wines, Michael, Sharon Lafraniere and Jonathan Ansfield. (2010, April 7). China's Censors Tackle and Trip Over the Internet. *The New York Times*.
Available at http://www.nytimes.com/2010/04/08/world/asia/08censor.html

India

For a full list of ISP in India, please visit -
http://www.trai.gov.in/Content/ProviderListDisp/3_ProviderListDisp.aspx

Xynou, Maria. (2014, January 30th). India's Central Monitoring System (CMS): Something to Worry About? The Centre for Internet and Society.
Available at http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

Freedom House. (2014). Freedom on the Net 2014.
Available at https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

Press Trust of India. (2014, February 12). Govt demands social networking sites to block 2,999 websites. The Business Standard. Available at http://www.business-standard.com/article/technology/govt-demands-social-networking-sites-to-block-1-299-websites-114021201126_1.html

Burke, Jason. (2015, March 24). India supreme court strikes down censorship law. The Guardian.
Available at http://www.theguardian.com/world/2015/mar/24/india-supreme-court-strikes-down-internet-censorship-law

Reporters without Borders. (2014). World Press Freedom Index.
Available at http://rsf.org/index2014/en-index2014.php

Indonesia

OpenNet Initiative. (2012). ONI Country Profile: Indonesia. *OpenNet Initiative*
Available at http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-indonesia.pdf

Freedom House. (2014). Freedom on the Net 2014: Indonesia. *Freedom House*.
Available at https://freedomhouse.org/report/freedom-net/2014/Indonesia

Gallagher, Sean. (2012, November 6). How an Indonesian ISP took down the mighty Google for 30 minutes. *Ars Technica Addendu*.
Available at http://arstechnica.com/information-technology/2012/11/how-an-indonesian-isp-took-down-the-mighty-google-for-30-minutes/

Croft-Cusworth, Catriona. (2014, May 16). Indonesia bans Vimeo. *The Interpreter.* Available at http://www.lowyinterpreter.org/post/2014/05/16/Indonesia-bans-Vimeo.aspx?COLLCC=1491902993&

Japan

Green, Chris. *Surviving in Japan.* Available at
http://www.survivingnjapan.com/2012/06/internet-in-japan-broadband-high-speed.html

U.S. Department of State. (2010). 2010 Human Rights Report: Japan. Government of the United States of America.
Available at http://www.state.gov/j/drl/rls/hrrpt/2010/eap/154386.htm

Myanmar

Freedom House. (2014). Freedom on the Net: Myanmar. *Freedom House*.
Available at https://freedomhouse.org/report/freedom-net/2014/myanmar

Greene Will. (2013, May 11). Myanmar's Promising Experiment with Internet Freedom. *Forbes.*
Available at http://www.forbes.com/sites/techonomy/2013/11/05/myanmars-promising-experiment-with-internet-freedom/

Herbert Smith (2012). Proposed new telecommunications law in Myanmar–where are the opportunities and risks for Japanese investors? *Intellectual Property & Technology, Media and Telecommunications newsletter* (19).
Available at http://www.herbertsmithfreehills.com/-/media/HS/T-240412-25.pdf

OpenNet Initiative. (2005). Internet Filtering in Burma in 2005: A Country Study, *OpenNet Initiative.*
Available at https://opennet.net/sites/opennet.net/files/ONI_Burma_Country_Study.pdf

Open Technology Fund (2013). Internet Access and Openness: Myanmar 2012, *Open Technology Fund and A Radio Free Asia Program.*
Available at https://www.opentechfund.org/files/reports/otf_myanmar_access_openness_public.pdf

Nepal

OpenNet Initiative. (2007). ONI Country Profile: Nepal. *OpenNet Initiative*

Available at https://opennet.net/research/profiles/nepal

North Korea

Fisher, Max. (2014, December 18). How North Korea, one of the world's poorest countries, got so good at hacking. *VOX*.
Available at http://www.vox.com/2014/12/18/7413229/north-korea-hack-sony

Fisher, Max. (2015, March 19). Yes, North Korea has the internet. Here's what it looks like. *VOX*.
Available at http://www.vox.com/2014/12/22/7435625/north-korea-internet

Frizell, Sam. (2014, December 22). North Korea Suffers Internet Blackout. *TIME*.
Available at http://time.com/3644632/north-korea-internet-sony/

Keck, Zachary. (2014, September 11). North Korea Bans Wi-Fi for Foreigners. *The Diplomat.*
Available at http://thediplomat.com/2014/09/north-korea-bans-wi-fi-for-foreigners/

Kim, Tong-Hyung and Youkyung Lee (2014, December 23). Look At How Bizarre North Korea's 'Internet' Is. *Business Insider*.
Available at http://www.businessinsider.com/a-look-at-north-koreas-tightly-controlled-internet-services-2014-12?IR=T

Lee, Dave. (2012, December 10). North Korea: On the net in world's most secretive nation. *BBC News.*
Available at http://www.bbc.com/news/technology-20445632

Sanger, David E. and Martin Fackler. (2015, January 18). N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say. *The New York Times*.
Available at http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

Sedaghat, Nouran. (2014, March 17). North Korea exposed: Censorship in the world's most secretive state. Canadian Journalists for Free Expression.
Available at https://cjfe.org/resources/features/north-korea-exposed-censorship-world%E2%80%99s-most-secretive-state

Sparkes, Matthew. (2014, December 23). Internet in North Korea: everything you need to know. The Telegraph.
Available at http://www.telegraph.co.uk/technology/11309882/Internet-in-North-Korea-everything-you-need-to-know.html

Pakistan

Hamdani, Yasser Latif. (2013). All Internet Censorship and Surveillance in Pakistan is Unconstitutional. *South Asia Jurist.*
Available at http://www.joomag.com/files_root/pdf/159861.pdf

Zhang, Qichen. (2012). Pakistan Plans to Step Up Censorship Before Elections. *OpenNet Initiative.*
Available at https://opennet.net/blog/2012/02/pakistan-plans-step-censorship-elections

South Korea

Electronic Frontiers Australia. (2003). Internet Censorship: Law & policy around the world. *Electronic Frontiers Australia.*
Available at https://www.efa.org.au/Issues/Censor/cens3.html#sk

The Economist. (2014, February 10). Why South Korea is really an internet dinosaur. *The Economist*.
Available at http://www.economist.com/blogs/economist-explains/2014/02/economist-explains-3

Freedom House. (2014). Freedom on the Net 2014: South Korea. *Freedom House*.
Available at https://freedomhouse.org/sites/default/files/resources/South%20Korea.pdf

Freedom House. (2012). Freedom on the Net 2012: South Korea. *Freedom House*.
Available at https://www.freedomhouse.org/sites/default/files/South%20Korea%202012.pdf

OpenNet Initiative. (2012). ONI Country Profile: South Korea. *OpenNet Initiative.*
Available at https://opennet.net/research/profiles/south-korea

Koo, Se-Woong. (2015, April 2). South Korea's invasion of privacy. The New York Times.
Available at http://www.nytimes.com/2015/04/03/opinion/south-koreas-invasion-of-privacy.html

Sri Lanka

BBC News. (2007, June 20). Popular Tamil website 'blocked', BBC News.
Available at http://news.bbc.co.uk/2/hi/south_asia/6221844.stm

Human Rights Watch. (2013, June 18). Sri Lanka: Proposed media code threatens free speech. *Human Rights Watch.*
Available at http://www.hrw.org/news/2013/06/18/sri-lanka-proposed-media-code-threatens-free-speech

Human Rights Watch. (2012, July 3). Sri Lanka: Halt Harassment of Media. *Human Rights Watch.*
Available at http://www.hrw.org/news/2012/07/03/sri-lanka-halt-harassment-media

Reporters Without Borders. Countries Under Surveillance: Sri Lanka. *Reporters Without Borders.*
Available at http://en.rsf.org/surveillance-sri-lanka,39720.html

Kumara, Sarath. (2010). Sri Lanka government prepares new internet restrictions. World Socialist Web Site. Available at http://www.wsws.org/en/articles/2010/02/slmd-f15.html

Thailand

Freedom House (2013). Freedom of Press, *Freedom House.*
Available at https://freedomhouse.org/report/freedom-press/2013/thailand#.VS-yFtyUfKM

Freedom House (2012). Freedom on the Net, *Freedom House.*
Available at https://freedomhouse.org/report/freedom-net/2012/thailand#.VS-xWtyUfKM

National Electronics and Computer Technology Center (2011). Thailand Information and Communication Technology Policy Framework (2011-2020), *Ministry of Information and Communication Technology.*
Available at http://www.mict.go.th/assets/portals/10/files/e-Publication/Executive%20Summary%20ICT2020.pdf